



Manage Cloud Volumes ONTAP

Cloud Manager

NetApp

September 09, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/concept_overview_cvo.html on September 09, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Manage Cloud Volumes ONTAP	1
Learn	1
Get started in AWS	38
Get started in Azure	90
Get started in GCP	112
Provision and manage storage	145
Manage storage VMs	174
Monitor performance	187
Improving protection against ransomware	194
Administer	196

Manage Cloud Volumes ONTAP

Learn

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 service to deliver backup and restore capabilities for protection, and long-term archive of your cloud data.

- 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.

- 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.



Licenses for ONTAP features are included with Cloud Volumes ONTAP.

[View supported Cloud Volumes ONTAP configurations](#)

[Learn more about Cloud Volumes ONTAP](#)

Storage

Disks and aggregates

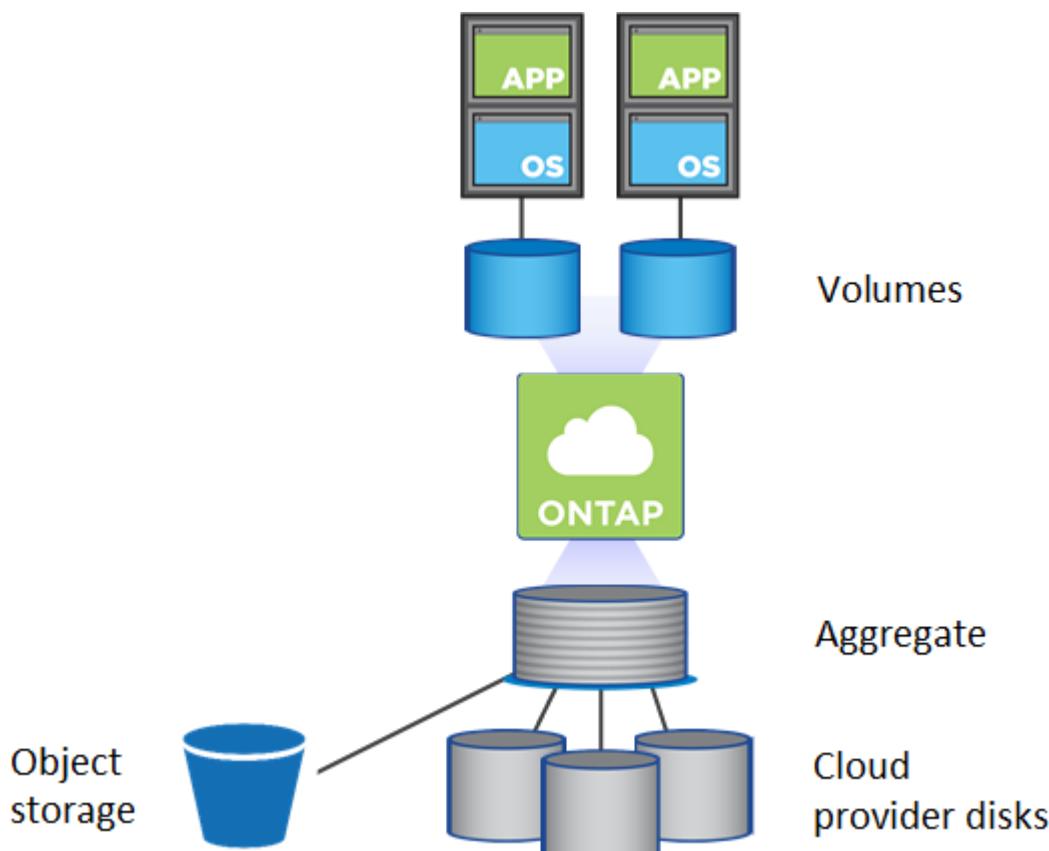
Understanding how Cloud Volumes ONTAP uses cloud storage can help you understand your storage costs.



All disks and aggregates must be created and deleted directly from Cloud Manager. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

Overview

Cloud Volumes ONTAP uses cloud provider storage as disks and groups them into one or more aggregates. Aggregates provide storage to one or more volumes.



Several types of cloud disks are supported. You choose the disk type when you create a volume and the default disk size when you deploy Cloud Volumes ONTAP.



The total amount of storage purchased from a cloud provider is the *raw capacity*. The *usable capacity* is less because approximately 12 to 14 percent is overhead that is reserved for Cloud Volumes ONTAP use. For example, if Cloud Manager creates a 500 GB aggregate, the usable capacity is 442.94 GB.

AWS storage

In AWS, Cloud Volumes ONTAP uses EBS storage for user data and local NVMe storage as Flash Cache on some EC2 instance types.

EBS storage

In AWS, an aggregate can contain up to 6 disks that are all the same size. The maximum disk size is 16 TB.

The underlying EBS disk type can be either General Purpose SSDs (gp3 or gp2), Provisioned IOPS SSD (io1), or Throughput Optimized HDD (st1). You can pair an EBS disk with Amazon S3 to [tier inactive data to low-cost object storage](#).



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

Local NVMe storage

Some EC2 instance types include local NVMe storage, which Cloud Volumes ONTAP uses as [Flash Cache](#).

Related links

- [AWS documentation: EBS Volume Types](#)
- [Learn how to choose disk types and disk sizes for your systems in AWS](#)
- [Review storage limits for Cloud Volumes ONTAP in AWS](#)
- [Review supported configurations for Cloud Volumes ONTAP in AWS](#)

Azure storage

In Azure, an aggregate can contain up to 12 disks that are all the same size. The disk type and maximum disk size depends on whether you use a single node system or an HA pair:

Single node systems

Single node systems can use three 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.

Each managed disk type has a maximum disk size of 32 TB.

You can pair a managed disk with Azure Blob storage to [tier inactive data to low-cost object storage](#).

HA pairs

HA pairs use Premium page blobs, which have a maximum disk size of 8 TB.

Related links

- [Microsoft Azure documentation: Introduction to Microsoft Azure Storage](#)
- [Learn how to choose disk types and disk sizes for your systems in Azure](#)
- [Review storage limits for Cloud Volumes ONTAP in Azure](#)

GCP storage

In GCP, an aggregate can contain up to 6 disks that are all the same size. The maximum disk size is 16 TB.

The disk type can be either *Zonal SSD persistent disks*, *Zonal Balanced persistent disks*, or *Zonal standard persistent disks*. You can pair persistent disks with a Google Storage bucket to [tier inactive data to low-cost object storage](#).

Related links

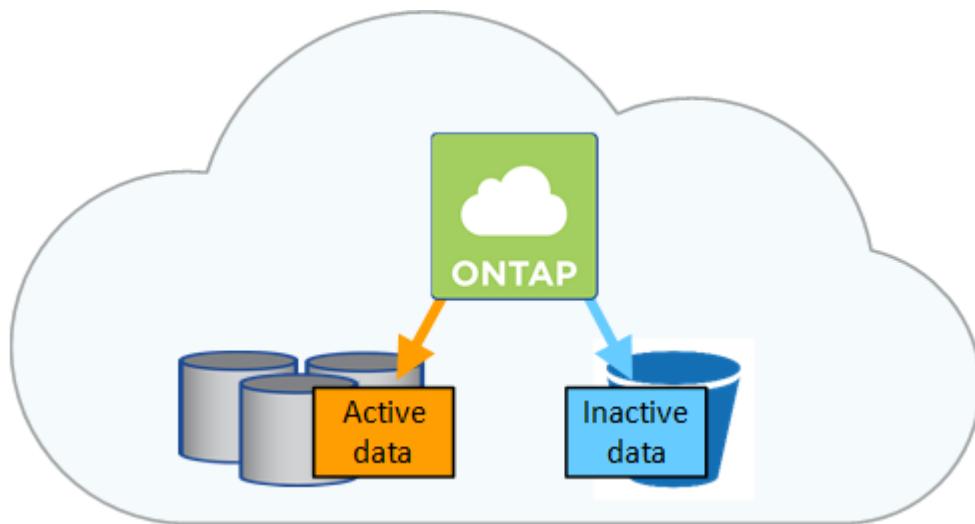
- [Google Cloud Platform documentation: Storage Options](#)
- [Review storage limits for Cloud Volumes ONTAP in GCP](#)

RAID type

The RAID type for each Cloud Volumes ONTAP aggregate is RAID0 (striping). No other RAID types are supported. Cloud Volumes ONTAP relies on the cloud provider for disk availability and durability.

Data tiering overview

Reduce your storage costs by enabling automated tiering of inactive data to low-cost object storage. Active data remains in high-performance SSDs or HDDs, while inactive data is tiered to low-cost object storage. This enables you to reclaim space on your primary storage and shrink secondary storage.



Cloud Volumes ONTAP supports data tiering in AWS, Azure, and Google Cloud Platform. Data tiering is powered by FabricPool technology.



You don't need to install a feature license to enable data tiering (FabricPool).

Data tiering in AWS

When you enable data tiering in AWS, Cloud Volumes ONTAP uses EBS as a performance tier for hot data and AWS S3 as a capacity tier for inactive data.

Performance tier

The performance tier can be General Purpose SSDs (gp3 or gp2) or Provisioned IOPS SSDs (io1).



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

Capacity tier

A Cloud Volumes ONTAP system tiers inactive data to a single S3 bucket using the *Standard* storage class. Standard is ideal for frequently accessed data stored across multiple Availability Zones.



Cloud Manager creates a single S3 bucket for each working environment and names it `fabric-pool-cluster unique identifier`. A different S3 bucket is not created for each volume.

Storage classes

The default storage class for tiered data in AWS is *Standard*. If you don't plan to access the inactive data, you can reduce your storage costs by changing the storage class to one of the following: *Intelligent Tiering*, *One-Zone Infrequent Access*, or *Standard-Infrequent Access*. When you change the storage class, inactive data starts in the Standard storage class and transitions to the storage class that you selected, if the data is not accessed after 30 days.

The access costs are higher if you do access the data, so take that into consideration before you change the storage class. [Learn more about Amazon S3 storage classes](#).

You can select a storage class when you create the working environment and you can change it any time after. For details about changing the storage class, see [Tiering inactive data to low-cost object storage](#).

The storage class for data tiering is system wide—it's not per volume.

Data tiering in Azure

When you enable data tiering in Azure, Cloud Volumes ONTAP uses Azure managed disks as a performance tier for hot data and Azure Blob storage as a capacity tier for inactive data.

Performance tier

The performance tier can be either SSDs or HDDs.

Capacity tier

A Cloud Volumes ONTAP system tiers inactive data to a single Blob container using the Azure *hot* storage tier. The hot tier is ideal for frequently accessed data.



Cloud Manager creates a new storage account with a single container for each Cloud Volumes ONTAP working environment. The name of the storage account is random. A different container is not created for each volume.

Storage access tiers

The default storage access tier for tiered data in Azure is the *hot* tier. If you don't plan to access the inactive data, you can reduce your storage costs by changing to the *cool* storage tier. When you change the storage tier, inactive data starts in the hot storage tier and transitions to the cool storage tier, if the data is not accessed after 30 days.

The access costs are higher if you do access the data, so take that into consideration before you change the storage tier. [Learn more about Azure Blob storage access tiers](#).

You can select a storage tier when you create the working environment and you can change it any time after. For details about changing the storage tier, see [Tiering inactive data to low-cost object storage](#).

The storage access tier for data tiering is system wide—it's not per volume.

Data tiering in GCP

When you enable data tiering in GCP, Cloud Volumes ONTAP uses persistent disks as a performance tier for hot data and a Google Cloud Storage bucket as a capacity tier for inactive data.

Performance tier

The performance tier can be either SSDs or HDDs (standard disks).

Capacity tier

A Cloud Volumes ONTAP system tiers inactive data to a single Google Cloud Storage bucket using the *Regional* storage class.



Cloud Manager creates a single bucket for each working environment and names it *fabric-pool-cluster unique identifier*. A different bucket is not created for each volume.

Storage classes

The default storage class for tiered data is the *Standard Storage* class. If the data is infrequently accessed, you can reduce your storage costs by changing to *Nearline Storage* or *Coldline Storage*. When you change the storage class, inactive data starts in the Standard Storage class and transitions to the storage class that you selected, if the data is not accessed after 30 days.

The access costs are higher if you do access the data, so take that into consideration before you change the storage class. [Learn more about storage classes for Google Cloud Storage](#).

You can select a storage tier when you create the working environment and you can change it any time after. For details about changing the storage class, see [Tiering inactive data to low-cost object storage](#).

The storage class for data tiering is system wide—it's not per volume.

Data tiering and capacity limits

If you enable data tiering, a system's capacity limit stays the same. The limit is spread across the performance tier and the capacity tier.

Volume tiering policies

To enable data tiering, you must select a volume tiering policy when you create, modify, or replicate a volume. You can select a different policy for each volume.

Some tiering policies have an associated minimum cooling period, which sets the time that user data in a volume must remain inactive for the data to be considered "cold" and moved to the capacity tier. The cooling period starts when data is written to the aggregate.



You can change the minimum cooling period and default aggregate threshold of 50% (more on that below). [Learn how to change the cooling period](#) and [learn how to change the threshold](#).

Cloud Manager enables you to choose from the following volume tiering policies when you create or modify a volume:

Snapshot Only

After an aggregate has reached 50% capacity, Cloud Volumes ONTAP tiers cold user data of Snapshot copies that are not associated with the active file system to the capacity tier. The cooling period is approximately 2 days.

If read, cold data blocks on the capacity tier become hot and are moved to the performance tier.

All

All data (not including metadata) is immediately marked as cold and tiered to object storage as soon as possible. There is no need to wait 48 hours for new blocks in a volume to become cold. Note that blocks located in the volume prior to the All policy being set require 48 hours to become cold.

If read, cold data blocks on the cloud tier stay cold and are not written back to the performance tier. This policy is available starting with ONTAP 9.6.

Auto

After an aggregate has reached 50% capacity, Cloud Volumes ONTAP tiers cold data blocks in a volume to a capacity tier. The cold data includes not just Snapshot copies but also cold user data from the active file system. The cooling period is approximately 31 days.

This policy is supported starting with Cloud Volumes ONTAP 9.4.

If read by random reads, the cold data blocks in the capacity tier become hot and move to the performance tier. If read by sequential reads, such as those associated with index and antivirus scans, the cold data blocks stay cold and do not move to the performance tier.

None

Keeps data of a volume in the performance tier, preventing it from being moved to the capacity tier.

When you replicate a volume, you can choose whether to tier the data to object storage. If you do, Cloud Manager applies the **Backup** policy to the data protection volume. Starting with Cloud Volumes ONTAP 9.6, the **All** tiering policy replaces the backup policy.

Turning off Cloud Volumes ONTAP impacts the cooling period

Data blocks are cooled by cooling scans. During this process, blocks that haven't been used have their block temperature moved (cooled) to the next lower value. The default cooling time depends on the volume tiering policy:

- Auto: 31 days
- Snapshot Only: 2 days

Cloud Volumes ONTAP must be running for the cooling scan to work. If Cloud Volumes ONTAP is turned off, cooling will stop, as well. As a result, you can experience longer cooling times.



When Cloud Volumes ONTAP is turned off, the temperature of each block is preserved until you restart the system. For example, if the temperature of a block is 5 when you turn the system off, the temp is still 5 when you turn the system back on.

Setting up data tiering

For instructions and a list of supported configurations, see [Tiering inactive data to low-cost object storage](#).

Storage management

Cloud Manager provides simplified and advanced management of Cloud Volumes ONTAP storage.



All disks and aggregates must be created and deleted directly from Cloud Manager. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

Storage provisioning

Cloud Manager makes storage provisioning for Cloud Volumes ONTAP easy by purchasing disks and managing aggregates for you. You simply need to create volumes. You can use an advanced allocation option to provision aggregates yourself, if desired.

Simplified provisioning

Aggregates provide cloud storage to volumes. Cloud Manager creates aggregates for you when you launch an instance, and when you provision additional volumes.

When you create a volume, Cloud Manager does one of three things:

- It places the volume on an existing aggregate that has sufficient free space.
- It places the volume on an existing aggregate by purchasing more disks for that aggregate.
- It purchases disks for a new aggregate and places the volume on that aggregate.

Cloud Manager determines where to place a new volume by looking at several factors: an aggregate's maximum size, whether thin provisioning is enabled, and free space thresholds for aggregates.



The Account Admin can modify free space thresholds from the **Settings** page.

Disk size selection for aggregates in AWS

When Cloud Manager creates new aggregates for Cloud Volumes ONTAP in AWS, it gradually increases the disk size in an aggregate, as the number of aggregates in the system increases. Cloud Manager does this to ensure that you can utilize the system's maximum capacity before it reaches the maximum number of data disks allowed by AWS.

For example, Cloud Manager might choose the following disk sizes for aggregates in a Cloud Volumes ONTAP Premium or BYOL system:

Aggregate number	Disk size	Max aggregate capacity
1	500 MB	3 TB
4	1 TB	6 TB
6	2 TB	12 TB

You can choose the disk size yourself by using the advanced allocation option.

Advanced allocation

Rather than let Cloud Manager manage aggregates for you, you can do it yourself. From the [Advanced allocation page](#), you can create new aggregates that include a specific number of disks, add disks to an existing aggregate, and create volumes in specific aggregates.

Capacity management

The Account Admin can choose whether Cloud Manager notifies you of storage capacity decisions or whether Cloud Manager automatically manages capacity requirements for you. It might help for you to understand how these modes work.

Automatic capacity management

The Capacity Management Mode is set to automatic by default. In this mode, Cloud Manager automatically purchases new disks for Cloud Volumes ONTAP instances when more capacity is needed, deletes unused collections of disks (aggregates), moves volumes between aggregates when needed, and attempts to unfail disks.

The following examples illustrate how this mode works:

- If an aggregate with 5 or fewer EBS disks reaches the capacity threshold, Cloud Manager automatically purchases new disks for that aggregate so volumes can continue to grow.
- If an aggregate with 12 Azure disks reaches the capacity threshold, Cloud Manager automatically moves a volume from that aggregate to an aggregate with available capacity or to a new aggregate.

If Cloud Manager creates a new aggregate for the volume, it chooses a disk size that accommodates the size of that volume.

Note that free space is now available on the original aggregate. Existing volumes or new volumes can use that space. The space can't be returned to AWS, Azure, or GCP in this scenario.

- If an aggregate contains no volumes for more than 12 hours, Cloud Manager deletes it.

Management of LUNs with automatic capacity management

Cloud Manager's automatic capacity management doesn't apply to LUNs. When Cloud Manager creates a LUN, it disables the autogrow feature.

Manual capacity management

If the Account Admin set the Capacity Management Mode to manual, Cloud Manager displays Action Required messages when capacity decisions must be made. The same examples described in the automatic mode apply to the manual mode, but it is up to you to accept the actions.

Write speed

Cloud Manager enables you to choose normal or high write speed 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.

High write speed is supported with all types of single node systems. It's also supported with HA pairs in AWS and Azure when using a specific instance or VM type (refer to the sections below for the list of supported

instances and VM types). High write speed is not supported with HA pairs in GCP.

Normal write speed

When you choose normal write speed, data is written directly to disk. When data is written directly to disk, reduces the likelihood of data loss in the event of an unplanned system outage, or a cascading failure involving an unplanned system outage (HA pairs only).

Normal write speed is the default option.

High write speed

When you choose high write speed, data is buffered in memory before it is written to disk, which provides faster write performance. Due to this caching, there is the potential for data loss if an unplanned system outage occurs.

The amount of data that can be lost in the event of an unplanned system outage is the span of the last two consistency points. A consistency point is the act of writing buffered data to disk. A consistency point occurs when the write log is full or after 10 seconds (whichever comes first). However, the performance of the storage provided by your cloud provider can affect consistency point processing time.

When to use high write speed

High write speed is a good choice if fast write performance is required for your workload and you can withstand the risk of data loss in the event of an unplanned system outage, or a cascading failure involving an unplanned system outage (HA pairs only).

Recommendations when using high write speed

If you enable high write speed, you should ensure write protection at the application layer, or that the applications can tolerate data loss, if it occurs.

Configurations that support high write speed

Not all Cloud Volumes ONTAP configurations support high write speed. Those configurations use normal write speed by default.

AWS

If you use a single node system, Cloud Volumes ONTAP supports high write speed with all instance types.

Starting with the 9.8 release, Cloud Volumes ONTAP supports high write speed with HA pairs when using almost all supported EC2 instance types, except for m5.xlarge and r5.xlarge.

[Learn more about the Amazon EC2 instances that Cloud Volumes ONTAP supports.](#)

Azure

If you use a single node system, Cloud Volumes ONTAP supports high write speed with all VM types.

If you use an HA pair, Cloud Volumes ONTAP supports high write speed with the following VM types, starting with the 9.8 release:

- DS5_v2

- DS14_v2
- DS15_v2
- E48s_v3

[Learn more about the Azure VM types that Cloud Volumes ONTAP supports.](#)

Google Cloud

If you use a single node system, Cloud Volumes ONTAP supports high write speed with all machine types.

Cloud Volumes ONTAP doesn't support high write speed with HA pairs in Google Cloud.

[Learn more about the Google Cloud machine types that Cloud Volumes ONTAP supports.](#)

How to select a write speed

You can choose a write speed when you create a new working environment and you can [change the write speed for an existing system](#).

What to expect if data loss occurs

If you choose high write speed and data loss occurs, the system should be able to boot up and continue to serve data without user intervention. Two EMS messages will be reported when a node runs into data loss. One is wafl.root.content.changed with the ERROR severity level event, the other is nv.check.failed with the DEBUG severity level event. Both messages must be present as an indication of data loss.

How to stop data access if data loss occurs

If you are concerned about data loss, want the applications to stop running upon data loss, and the data access to be resumed after the data loss issue is properly addressed, you can use the NVFAIL option from the CLI to achieve that goal.

To enable the NVFAIL option

```
vol modify -volume <vol-name> -nvfail on
```

To check NVFAIL settings

```
vol show -volume <vol-name> -fields nvfail
```

To disable the NVFAIL option

```
vol modify -volume <vol-name> -nvfail off
```

When data loss occurs, an NFS or iSCSI volume with NVFAIL enabled should stop serving data (there's no impact to CIFS which is a stateless protocol). For more details, refer to [How NVFAIL impacts access to NFS volumes or LUNs](#).

To check the NVFAIL state

```
vol show -fields in-nvfailed-state
```

After the data loss issue is properly addressed, you can clear the NVFAIL state and the volume will be available for data access.

To clear the NVFAIL state

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

Flash Cache

Some Cloud Volumes ONTAP configurations in AWS and Azure include local NVMe storage, which Cloud Volumes ONTAP uses as *Flash Cache* for better performance.

What's Flash Cache?

Flash Cache speeds access to data through real-time intelligent caching of recently read user data and NetApp metadata. It's effective for random read-intensive workloads, including databases, email, and file services.

Supported instances in AWS

Select one of the following EC2 instance types with a new or existing Cloud Volumes ONTAP Premium or BYOL system:

- c5d.4xlarge
- c5d.9xlarge
- c5d.18xlarge
- m5d.8xlarge
- m5d.12xlarge
- r5d.2xlarge

Supported VM type in Azure

Select the Standard_L8s_v2 VM type with a single node Cloud Volumes ONTAP BYOL system in Azure.

Limitations

- Compression must be disabled on all volumes to take advantage of the Flash Cache performance improvements.

Choose no storage efficiency when creating a volume from Cloud Manager, or create a volume and then [disable data compression by using the CLI](#).

- Cache rewarming after a reboot is not supported with Cloud Volumes ONTAP.

WORM storage

You can activate write once, read many (WORM) storage on a Cloud Volumes ONTAP system to retain files in unmodified form for a specified retention period. WORM storage is powered by SnapLock technology in Enterprise mode, which means WORM files are protected at the file level.

Once a file has been committed to WORM storage, it can't be modified, even after the retention period has expired. A tamper-proof clock determines when the retention period for a WORM file has elapsed.

After the retention period has elapsed, you are responsible for deleting any files that you no longer need.

Activating WORM storage

You can activate WORM storage on a Cloud Volumes ONTAP system when you create a new working environment. This includes setting the default retention period for files.



You can't activate WORM storage on individual volumes—WORM must be activated at the system level.

The following image shows how to activate WORM storage when creating a working environment:

Create a New Working Environment WORM (write once, read many)

↑ Previous Step Write Speed

Normal
Data is written directly to disk, reducing the likelihood of data loss in the event of an unplanned system outage.

High
Data is buffered in memory before it is written to disk, which provides faster write performance. Due to this caching, there is the potential for data loss in the event of an unplanned system outage.

WORM

You can use write once, read many (WORM) storage to retain critical files in unmodified form for regulatory and governance purposes and to protect from malware attacks. WORM files are protected at the file level.
[Learn More](#)

Disable WORM Activate WORM

Notice: If you activate WORM storage, data tiering to object storage will be disabled on the system.

Retention Period 15 years

Cloud Manager 3.9.9 Build: 0 Jun 30, 2021 02:52:27 pm UTC Environment: staging

Committing files to WORM

You can use an application to commit files to WORM over NFS or CIFS, or use the ONTAP CLI to autocommit files to WORM automatically. You can also use a WORM appendable file to retain data that is written incrementally, like log information.

After you activate WORM storage on a Cloud Volumes ONTAP system, you must use the ONTAP CLI for all management of WORM storage. For instructions, refer to [ONTAP documentation](#).



Cloud Volumes ONTAP support for WORM storage is equivalent to SnapLock Enterprise mode.

Limitations

- WORM storage in Cloud Volumes ONTAP operates under a "trusted storage administrator" model. While WORM files are protected from alteration or modification, volumes can be deleted by a cluster administrator even if those volumes contain unexpired WORM data.
- In addition to the trusted storage administrator model, WORM storage in Cloud Volumes ONTAP also implicitly operates under a "trusted cloud administrator" model. A cloud administrator could delete WORM data before its expiry date by removing or editing cloud storage directly from the cloud provider.
- When WORM storage is activated, data tiering to object storage can't be enabled.
- Cloud Backup must be disabled in order to enable WORM storage.

High-availability pairs

High-availability pairs in AWS

A Cloud Volumes ONTAP high availability (HA) configuration provides nondisruptive operations and fault tolerance. In AWS, data is synchronously mirrored between the two nodes.

Overview

In AWS, Cloud Volumes ONTAP HA configurations include the following components:

- Two Cloud Volumes ONTAP nodes whose data is synchronously mirrored between each other.
- A mediator instance that provides a communication channel between the nodes to assist in storage takeover and giveback processes.



The mediator instance runs the Linux operating system on a t2.micro instance and uses one EBS magnetic disk that is approximately 8 GB.

Storage takeover and giveback

If a node goes down, the other node can serve data for its partner to provide continued data service. Clients can access the same data from the partner node because the data was synchronously mirrored to the partner.

After the node reboots, the partner must resync data before it can return the storage. The time that it takes to resync data depends on how much data was changed while the node was down.

Storage takeover, resync, and giveback are all automatic by default. No user action is required.

RPO and RTO

An HA configuration maintains high availability of your data as follows:

- The recovery point objective (RPO) is 0 seconds.
Your data is transactionally consistent with no data loss.
- The recovery time objective (RTO) is 60 seconds.
In the event of an outage, data should be available in 60 seconds or less.

HA deployment models

You can ensure the high availability of your data by deploying an HA configuration across multiple Availability Zones (AZs) or in a single AZ. You should review more details about each configuration to choose which best fits your needs.

Multiple Availability Zones

Deploying an HA configuration in multiple Availability Zones (AZs) ensures high availability of your data if a failure occurs with an AZ or an instance that runs a Cloud Volumes ONTAP node. You should understand how NAS IP addresses impact data access and storage failover.

NFS and CIFS data access

When an HA configuration is spread across multiple Availability Zones, *floating IP addresses* enable NAS client access. The floating IP addresses, which must be outside of the CIDR blocks for all VPCs in the region, can migrate between nodes when failures occur. They aren't natively accessible to clients that are outside of the VPC, unless you [set up an AWS transit gateway](#).

If you can't set up a transit gateway, private IP addresses are available for NAS clients that are outside the VPC. However, these IP addresses are static—they can't failover between nodes.

You should review requirements for floating IP addresses and route tables before you deploy an HA configuration across multiple Availability Zones. You must specify the floating IP addresses when you deploy the configuration. The private IP addresses are automatically created by Cloud Manager.

For details, see [AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs](#).

iSCSI data access

Cross-VPC data communication is not an issue since iSCSI does not use floating IP addresses.

Takeover and giveback for iSCSI

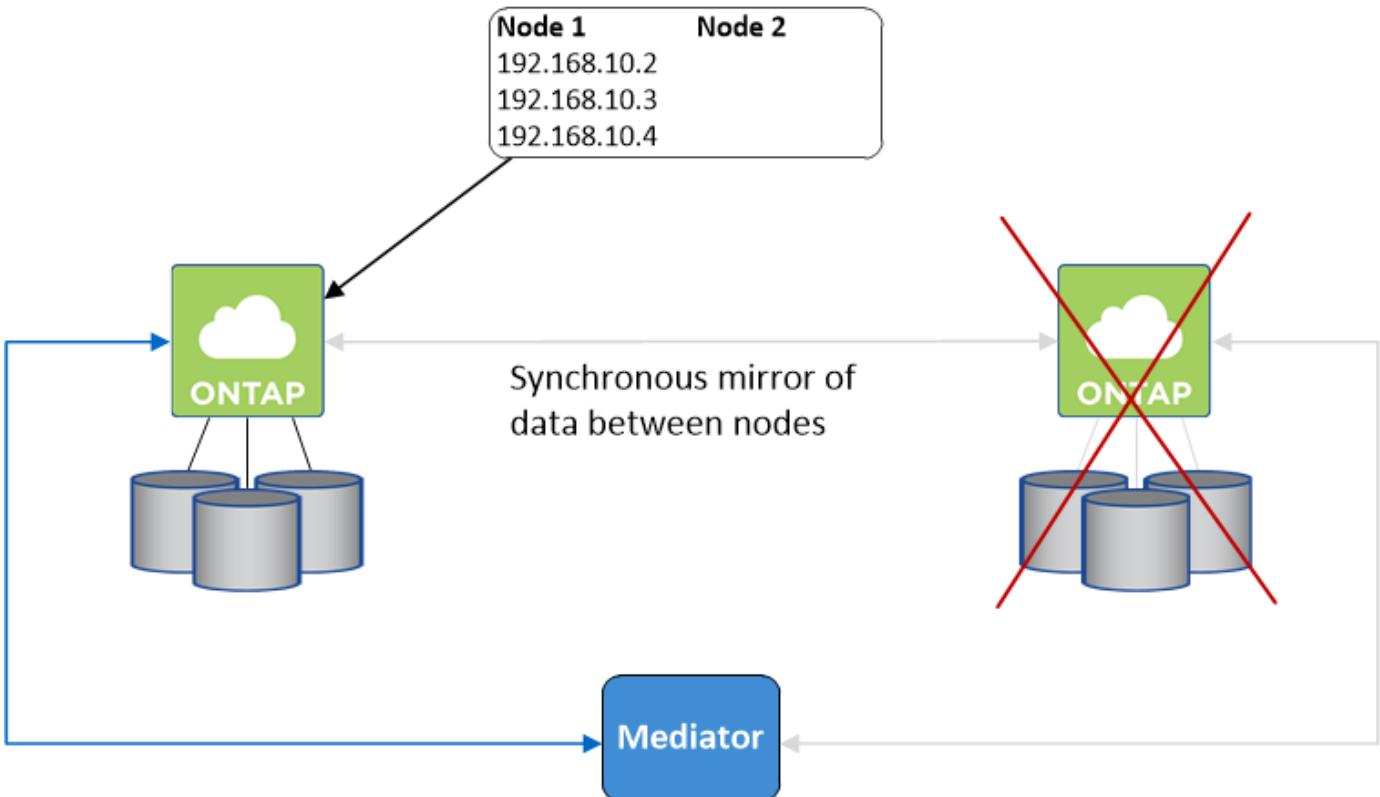
For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



For information about which specific host configurations support ALUA, see the [NetApp Interoperability Matrix Tool](#) and the Host Utilities Installation and Setup Guide for your host operating system.

Takeover and giveback for NAS

When takeover occurs in a NAS configuration using floating IPs, the node's floating IP address that clients use to access data moves to the other node. The following image depicts storage takeover in a NAS configuration using floating IPs. If node 2 goes down, the floating IP address for node 2 moves to node 1.



NAS data IPs used for external VPC access cannot migrate between nodes if failures occur. If a node goes offline, you must manually remount volumes to clients outside the VPC by using the IP address on the other node.

After the failed node comes back online, remount clients to volumes using the original IP address. This step is needed to avoid transferring unnecessary data between two HA nodes, which can cause significant performance and stability impact.

You can easily identify the correct IP address from Cloud Manager by selecting the volume and clicking **Mount Command**.

Cloud Volumes ONTAP HA in a single Availability Zone

Deploying an HA configuration in a single Availability Zone (AZ) can ensure high availability of your data if an instance that runs a Cloud Volumes ONTAP node fails. All data is natively accessible from outside of the VPC.



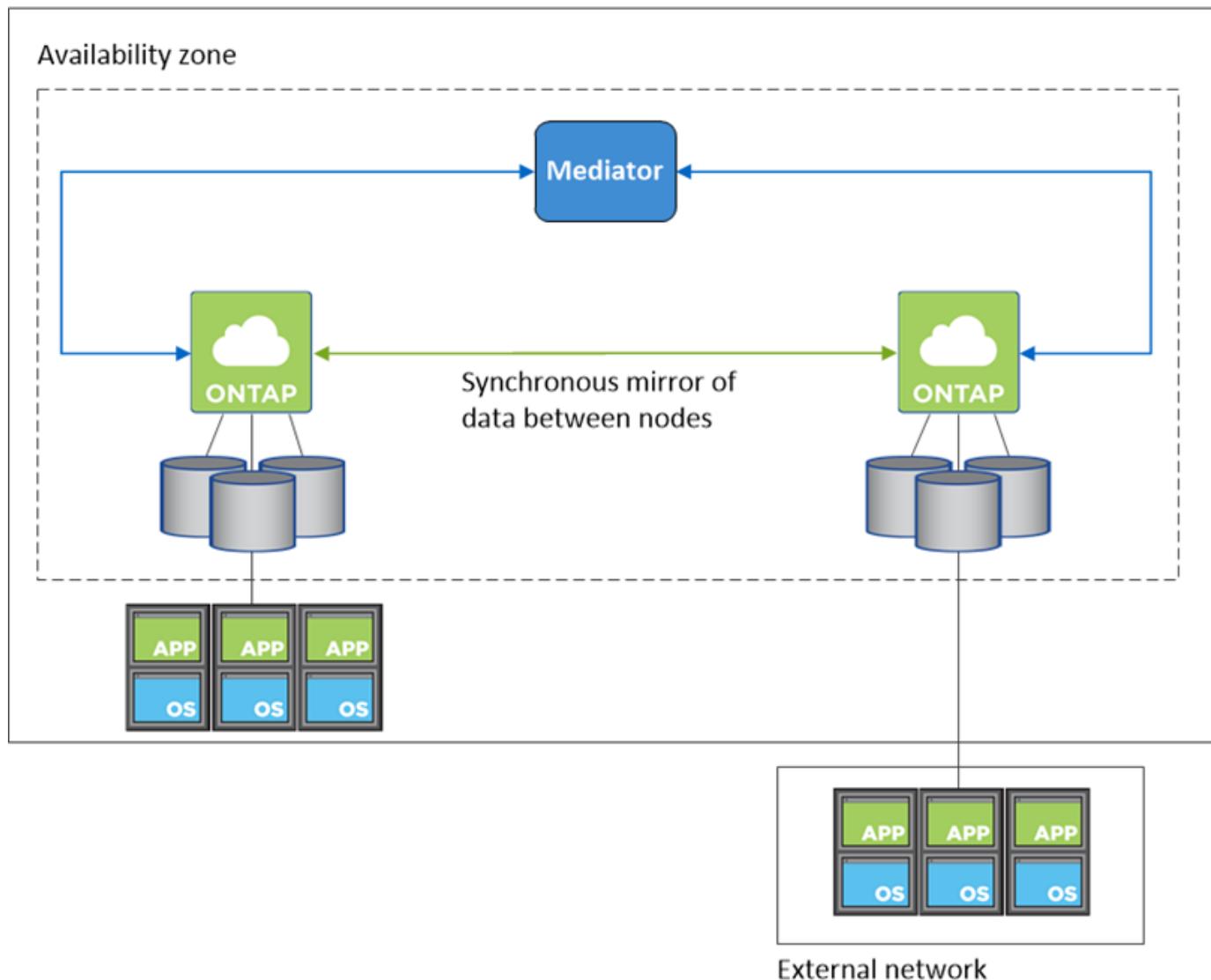
Cloud Manager creates an [AWS spread placement group](#) and launches the two HA nodes in that placement group. The placement group reduces the risk of simultaneous failures by spreading the instances across distinct underlying hardware. This feature improves redundancy from a compute perspective and not from disk failure perspective.

Data access

Because this configuration is in a single AZ, it does not require floating IP addresses. You can use the same IP address for data access from within the VPC and from outside the VPC.

The following image shows an HA configuration in a single AZ. Data is accessible from within the VPC and from outside the VPC.

VPC in AWS



Takeover and giveback

For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



For information about which specific host configurations support ALUA, see the [NetApp Interoperability Matrix Tool](#) and the Host Utilities Installation and Setup Guide for your host operating system.

For NAS configurations, the data IP addresses can migrate between HA nodes if failures occur. This ensures client access to storage.

How storage works in an HA pair

Unlike an ONTAP cluster, storage in a Cloud Volumes ONTAP HA pair is not shared between nodes. Instead, data is synchronously mirrored between the nodes so that the data is available in the event of failure.

Storage allocation

When you create a new volume and additional disks are required, Cloud Manager allocates the same number of disks to both nodes, creates a mirrored aggregate, and then creates the new volume. For example, if two disks are required for the volume, Cloud Manager allocates two disks per node for a total of four disks.

Storage configurations

You can use an HA pair as an active-active configuration, in which both nodes serve data to clients, or as an active-passive configuration, in which the passive node responds to data requests only if it has taken over storage for the active node.



You can set up an active-active configuration only when using Cloud Manager in the Storage System View.

Performance expectations

A Cloud Volumes ONTAP HA configuration synchronously replicates data between nodes, which consumes network bandwidth. As a result, you can expect the following performance in comparison to a single-node Cloud Volumes ONTAP configuration:

- For HA configurations that serve data from only one node, read performance is comparable to the read performance of a single-node configuration, whereas write performance is lower.
- For HA configurations that serve data from both nodes, read performance is higher than the read performance of a single-node configuration, and write performance is the same or higher.

For more details about Cloud Volumes ONTAP performance, see [Performance](#).

Client access to storage

Clients should access NFS and CIFS volumes by using the data IP address of the node on which the volume resides. If NAS clients access a volume by using the IP address of the partner node, traffic goes between both nodes, which reduces performance.

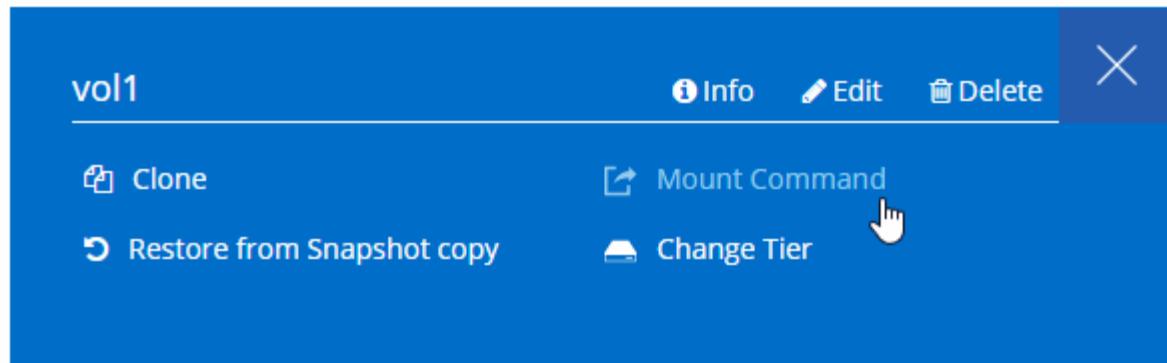


If you move a volume between nodes in an HA pair, you should remount the volume by using the IP address of the other node. Otherwise, you can experience reduced performance. If clients support NFSv4 referrals or folder redirection for CIFS, you can enable those features on the Cloud Volumes ONTAP systems to avoid remounting the volume. For details, see ONTAP documentation.

You can easily identify the correct IP address from Cloud Manager:

Volumes

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

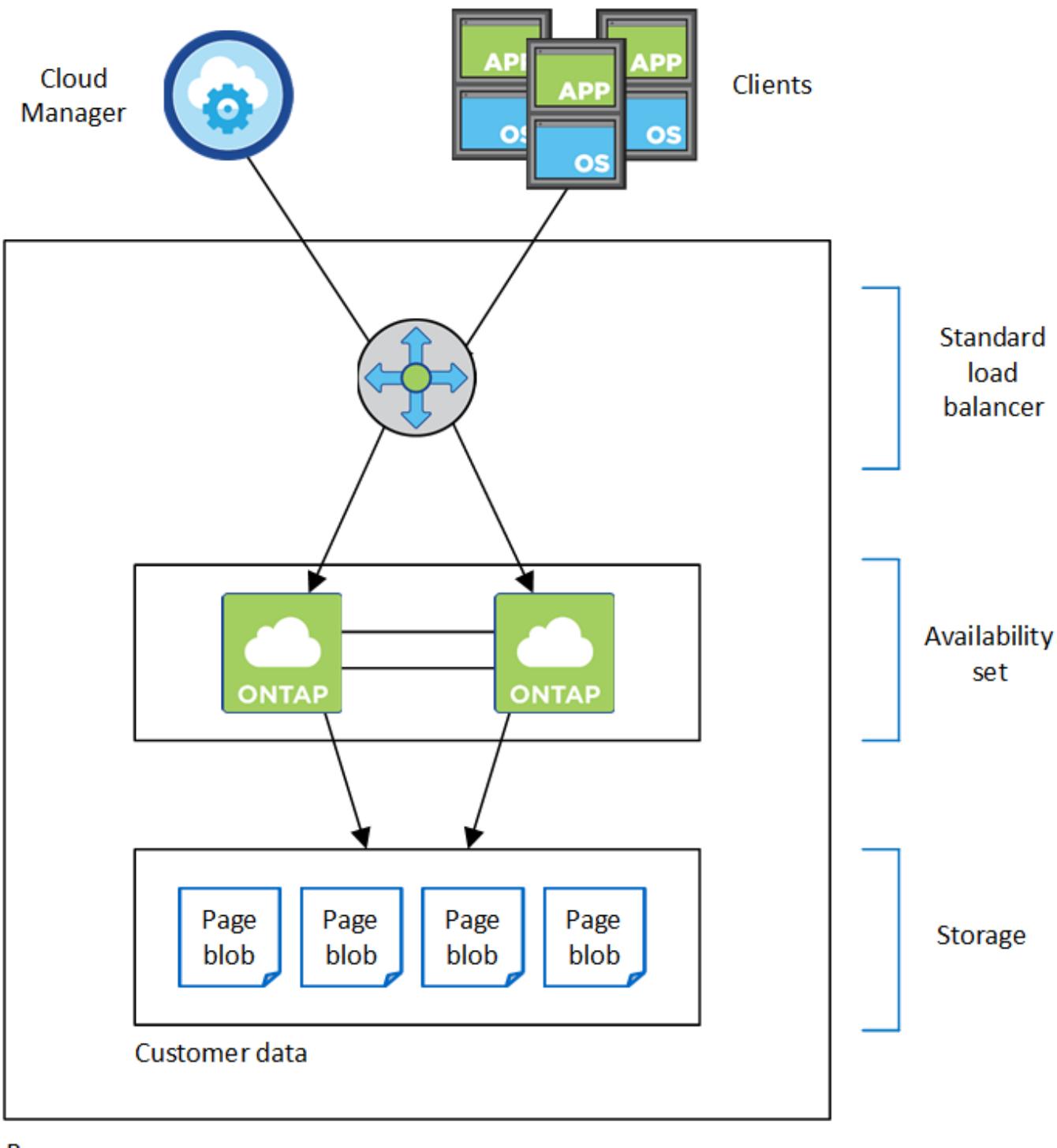


High-availability pairs in Azure

A Cloud Volumes ONTAP high availability (HA) pair provides enterprise reliability and continuous operations in case of failures in your cloud environment. In Azure, storage is shared between the two nodes.

HA components

A Cloud Volumes ONTAP HA configuration in Azure includes the following components:



Resource group

Note the following about the Azure components that Cloud Manager deploys for you:

Azure Standard Load Balancer

The load balancer manages incoming traffic to the Cloud Volumes ONTAP HA pair.

Availability Set

The Azure Availability Set is a logical grouping of the Cloud Volumes ONTAP nodes. The Availability Set ensures that the nodes are in different fault and update domains to provide redundancy and availability. [Learn more about Availability Sets in the Azure docs.](#)

Disks

Customer data resides on Premium Storage page blobs. Each node has access to the other node's storage. Additional storage is also required for [boot, root, and core data](#).

Storage accounts

- One storage account is required for managed disks.
- One or more storage accounts are required for the Premium Storage page blobs, as the disk capacity limit per storage account is reached.

[Azure documentation: Azure Storage scalability and performance targets for storage accounts](#).

- One storage account is required for data tiering to Azure Blob storage.
- Starting with Cloud Volumes ONTAP 9.7, the storage accounts that Cloud Manager creates for HA pairs are general-purpose v2 storage accounts.
- You can enable an HTTPS connection from a Cloud Volumes ONTAP 9.7 HA pair to Azure storage accounts when creating a working environment. Note that enabling this option can impact write performance. You can't change the setting after you create the working environment.

RPO and RTO

An HA configuration maintains high availability of your data as follows:

- The recovery point objective (RPO) is 0 seconds.
Your data is transactionally consistent with no data loss.
- The recovery time objective (RTO) is 60 seconds.
In the event of an outage, data should be available in 60 seconds or less.

Storage takeover and giveback

Similar to a physical ONTAP cluster, storage in an Azure HA pair is shared between nodes. Connections to the partner's storage allows each node to access the other's storage in the event of a *takeover*. Network path failover mechanisms ensure that clients and hosts continue to communicate with the surviving node. The partner *gives back* storage when the node is brought back on line.

For NAS configurations, data IP addresses automatically migrate between HA nodes if failures occur.

For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



For information about which specific host configurations support ALUA, see the [NetApp Interoperability Matrix Tool](#) and the Host Utilities Installation and Setup Guide for your host operating system.

Storage takeover, resync, and giveback are all automatic by default. No user action is required.

Storage configurations

You can use an HA pair as an active-active configuration, in which both nodes serve data to clients, or as an active-passive configuration, in which the passive node responds to data requests only if it has taken over storage for the active node.

HA limitations

The following limitations affect Cloud Volumes ONTAP HA pairs in Azure:

- HA pairs are supported with Cloud Volumes ONTAP Standard, Premium, and BYOL. Explore is not supported.
- NFSv4 is not supported. NFSv3 is supported.
- HA pairs are not supported in some regions.

[See the list of supported Azure regions.](#)

[Learn how to deploy an HA system in Azure.](#)

High-availability pairs in Google Cloud Platform

A Cloud Volumes ONTAP high availability (HA) configuration provides nondisruptive operations and fault tolerance. In Google Cloud Platform, data is synchronously mirrored between the two nodes.

HA components

Cloud Volumes ONTAP HA configurations in GCP include the following components:

- Two Cloud Volumes ONTAP nodes whose data is synchronously mirrored between each other.
- A mediator instance that provides a communication channel between the nodes to assist in storage takeover and giveback processes.

The mediator runs the Linux operating system on a f1-micro instance and uses two standard persistent disks that are 10 GB each.

- One zone or three zones (recommended).

If you choose three zones, the two nodes and mediator are in separate Google Cloud zones.

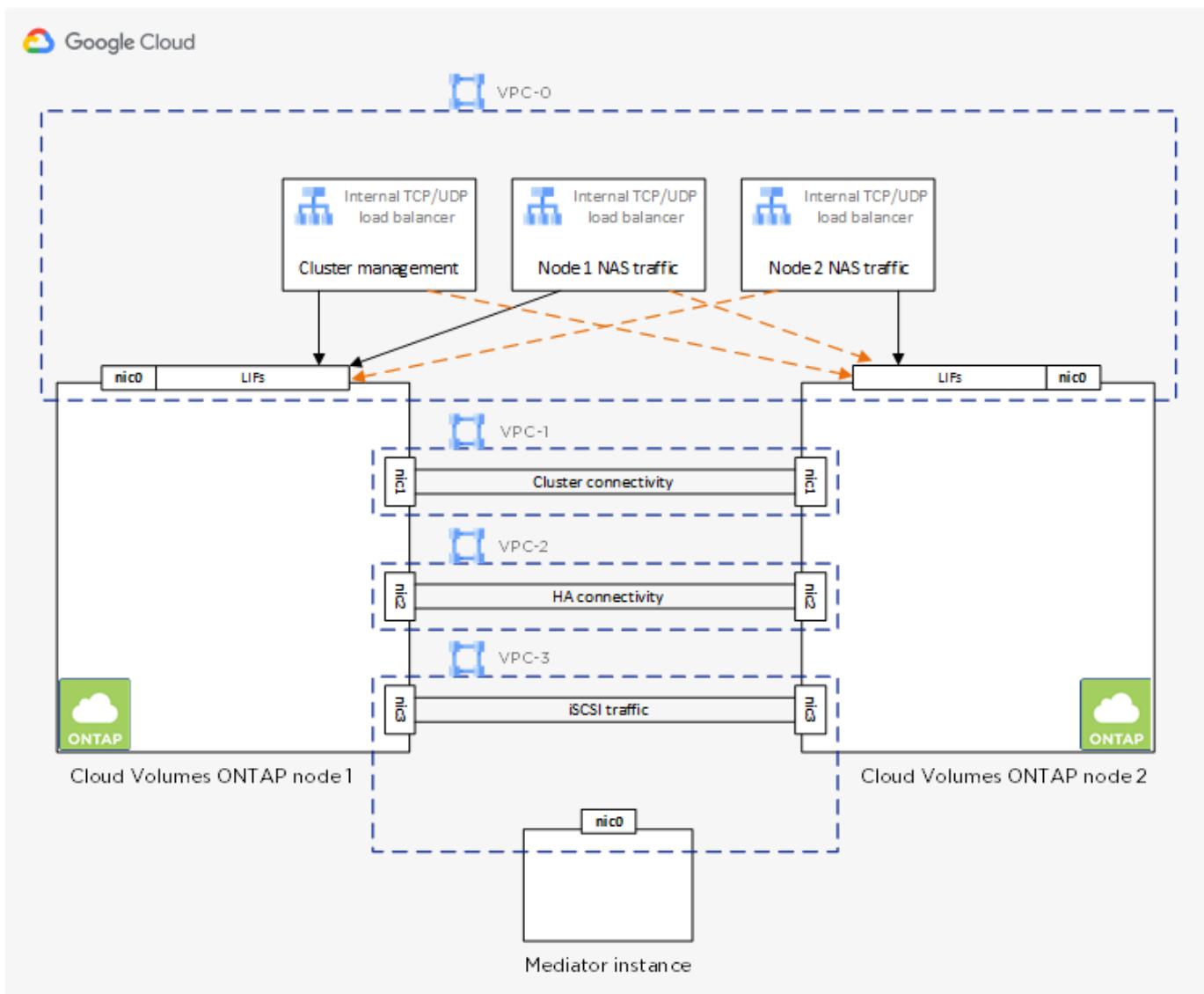
- Four Virtual Private Clouds (VPCs).

The configuration uses four VPCs because GCP requires that each network interface resides in a separate VPC network.

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

[Learn about networking requirements](#), including more details about load balancers, VPCs, internal IP addresses, subnets, and more.

The following conceptual image shows a Cloud Volumes ONTAP HA pair and its components:



Storage takeover and giveback

If a node goes down, the other node can serve data for its partner to provide continued data service. Clients can access the same data from the partner node because the data was synchronously mirrored to the partner.

After the node reboots, the partner must resync data before it can return the storage. The time that it takes to resync data depends on how much data was changed while the node was down.

Storage takeover, resync, and giveback are all automatic by default. No user action is required.

RPO and RTO

An HA configuration maintains high availability of your data as follows:

- The recovery point objective (RPO) is 0 seconds.

Your data is transactionally consistent with no data loss.

- The recovery time objective (RTO) is 60 seconds.

In the event of an outage, data should be available in 60 seconds or less.

HA deployment models

You can ensure the high availability of your data by deploying an HA configuration in multiple zones or in a single zone.

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.

How storage works in an HA pair

Unlike an ONTAP cluster, storage in a Cloud Volumes ONTAP HA pair in GCP is not shared between nodes. Instead, data is synchronously mirrored between the nodes so that the data is available in the event of failure.

Storage allocation

When you create a new volume and additional disks are required, Cloud Manager allocates the same number of disks to both nodes, creates a mirrored aggregate, and then creates the new volume. For example, if two disks are required for the volume, Cloud Manager allocates two disks per node for a total of four disks.

Storage configurations

You can use an HA pair as an active-active configuration, in which both nodes serve data to clients, or as an active-passive configuration, in which the passive node responds to data requests only if it has taken over storage for the active node.

Performance expectations for an HA configuration

A Cloud Volumes ONTAP HA configuration synchronously replicates data between nodes, which consumes network bandwidth. As a result, you can expect the following performance in comparison to a single-node Cloud Volumes ONTAP configuration:

- For HA configurations that serve data from only one node, read performance is comparable to the read performance of a single-node configuration, whereas write performance is lower.
- For HA configurations that serve data from both nodes, read performance is higher than the read performance of a single-node configuration, and write performance is the same or higher.

For more details about Cloud Volumes ONTAP performance, see [Performance](#).

Client access to storage

Clients should access NFS and CIFS volumes by using the data IP address of the node on which the volume resides. If NAS clients access a volume by using the IP address of the partner node, traffic goes between both nodes, which reduces performance.

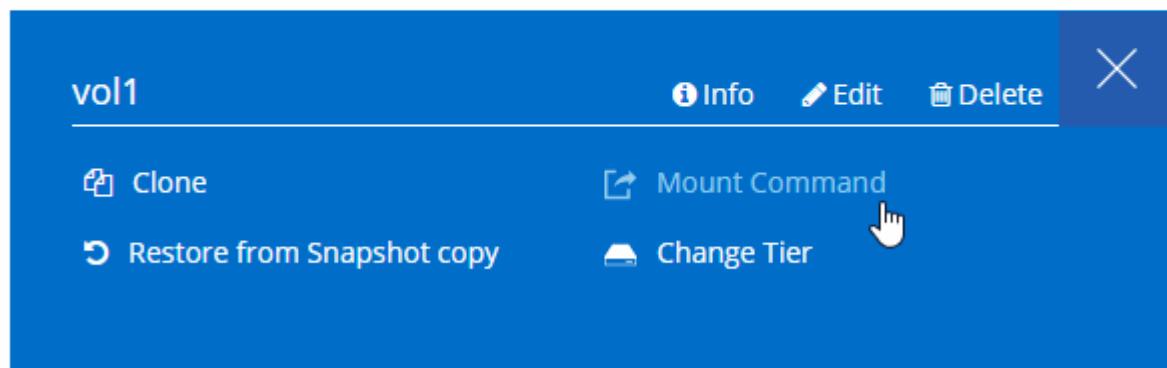
!

If you move a volume between nodes in an HA pair, you should remount the volume by using the IP address of the other node. Otherwise, you can experience reduced performance. If clients support NFSv4 referrals or folder redirection for CIFS, you can enable those features on the Cloud Volumes ONTAP systems to avoid remounting the volume. For details, see ONTAP documentation.

You can easily identify the correct IP address from Cloud Manager:

Volumes

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



Related links

- [Learn about networking requirements](#)
- [Learn how to get started in GCP](#)

Cloud Volumes ONTAP licensing

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

Licensing overview

The following table provides an overview of the licensing options for Cloud Volumes ONTAP.

Beyond these licensing options, you can also choose the *Freemium* offering to get started with Cloud Volumes ONTAP without purchasing a license or contract.

Charging method	Highlights	Support	Max system capacity
Capacity-based license: Essentials package	<ul style="list-style-type: none"> • Pay per TiB of capacity for one or more Cloud Volumes ONTAP systems • Provides a la carte licensing for Cloud Volumes ONTAP: <ul style="list-style-type: none"> ◦ A single node or HA system ◦ File and block storage or secondary data (DR) • Available by bringing your own license (BYOL) purchased from NetApp 	Included	2 PB
Capacity-based license: Professional package	<ul style="list-style-type: none"> • Pay per TiB of capacity for one or more Cloud Volumes ONTAP systems • Provides licensing for any Cloud Volumes ONTAP configuration (single node or HA with any storage type) • Includes volume backups using the Cloud Backup Service (only for volumes charged against this license) • Available through an AWS Marketplace annual contract or by bringing your own license (BYOL) purchased from NetApp 	Included	2 PB
PAYGO by node	<ul style="list-style-type: none"> • Pay-as-you-go by the hour through a marketplace subscription from your cloud provider • Charging is per Cloud Volumes ONTAP node • Available in three licensing options: Explore, Standard, and Premium 	Included, but you must activate support	<ul style="list-style-type: none"> • Explore: 2 TB • Standard: 10 TB • Premium: 368 TB
Node-based license	<ul style="list-style-type: none"> • Single node or HA license with term-based options • Available by bringing your own license (BYOL) purchased from NetApp 	Included	368 TB per license

The following sections provide more details about each of these options.

Freemium offering

- A new offering that provides all Cloud Volumes ONTAP features free of charge from NetApp (cloud provider charges still apply).
- No license or contract is needed.
- Support is not included.

- You're limited to 500 GB of provisioned capacity per Cloud Volumes ONTAP system.
- You can use up to 10 Cloud Volumes ONTAP systems with the Freemium offering per NetApp account.
- If the provisioned capacity for a Cloud Volumes ONTAP system exceeds 500 GB, Cloud Manager converts the system to the Essentials package (which is a capacity-based license) and charging starts.

Any other systems that have less than 500 GB of provisioned capacity stay on the Freemium offering (as long as they were deployed using the Freemium offering).

To get started with the Freemium offering, create a new Cloud Volumes ONTAP working environment and select **Freemium** when prompted to choose a charging method.

Capacity-based licenses

Capacity-based licensing enables you to pay for Cloud Volumes ONTAP per TiB of capacity. The license is associated with your NetApp account and enables you to charge multiple systems against the license, as long as enough capacity is available through the license.

For example, you could purchase a single 20 TB license, deploy four Cloud Volumes ONTAP systems, and then allocate a 5 TB volume to each system, for a total of 20 TB.

Unlike the by-node charging method where a license is purchased per Cloud Volumes ONTAP system, a capacity-based license is issued to a NetApp account. The capacity is then available to the volumes on each Cloud Volumes ONTAP system deployed in that account.

Capacity-based licensing is available in the form of a *package*. When you deploy a Cloud Volumes ONTAP system, you can choose from the following packages: Essentials or Professional.

This licensing method is available for Cloud Volumes ONTAP 9.7 and later.



For each package, there is a minimum 4 TB capacity charge. Any Cloud Volumes ONTAP instance that has less than 4 TB of capacity will be charged at a rate of 4 TB.

Essentials package

- Provides a la carte licensing for Cloud Volumes ONTAP:
 - A single node or HA system
 - File and block storage or secondary data for disaster recovery (DR)
- This package is available as a license (BYOL) purchased from NetApp.
- Support is included for the length of the subscription term.
- Conversions to another licensing option isn't supported.
- Each individual Cloud Volumes ONTAP system supports up to 2 PB of capacity through disks and tiering to object storage.

Professional package

- Provides licensing for any Cloud Volumes ONTAP configuration (single node or HA with any storage type).
- Includes volume backups using the Cloud Backup Service (only for volumes charged against this license).
- This package is available as an annual contract from the AWS Marketplace or as a license (BYOL) purchased from NetApp.

If you have an AWS Marketplace contract, *all* Cloud Volumes ONTAP systems that you deploy are charged against that contract. You can't mix and match a Marketplace contract with BYOL.

- Support is included for the length of the subscription term.
- Conversions to another licensing option isn't supported.
- Each individual Cloud Volumes ONTAP system supports up to 2 PB of capacity through disks and tiering to object storage.

To get started with a capacity-based license, [Contact NetApp Sales](#) and then [add your license to Cloud Manager](#).

PAYGO by node

- Requires a subscription from a cloud provider's marketplace for pay-as-you-go pricing at an hourly rate.
- Charging is per Cloud Volumes ONTAP node.
- Offers Cloud Volumes ONTAP in three different licensing options: Explore, Standard, and Premium. Each license provides support for different amounts of storage and compute.
- A 30-day free trial is available for the first Cloud Volumes ONTAP system that you deploy in a cloud provider. [Learn more about 30-day free trials](#).
 - There are no hourly software charges, but cloud provider infrastructure charges still apply (compute, storage, and networking).
 - When the free trial ends, you'll be charged hourly according to the selected license, as long as you subscribed. If you haven't subscribed, the system shuts down.

Cloud Manager prompts you to subscribe to your cloud provider's marketplace when you create a Cloud Volumes ONTAP system.

- Conversions to another licensing option isn't supported.
- Basic technical support is offered, but you must [register and activate the NetApp serial number associated with your system](#).

You can view pricing details from your cloud provider's marketplace:

- [AWS Marketplace](#)
- [Azure Marketplace](#)
- [Google Cloud Platform Marketplace](#)

To get started with PAYGO, create a Cloud Volumes ONTAP working environment and subscribe to your cloud provider's marketplace when prompted.

Node-based licenses

- Single node or HA license with term-based subscription options like 12 months, 24 months, and more.
- Available by bringing your own license (BYOL) purchased from NetApp.
- Each Cloud Volumes ONTAP system supports up to 368 TB of capacity per license.
- Conversions to another licensing option isn't supported.

If you want to transition to capacity-based licensing, you can purchase a license, deploy a new Cloud Volumes ONTAP system, and then replicate the data to that new system.

To get started with a node-based license, [Contact NetApp Sales](#) and then [add your license to Cloud Manager](#).

License management for node-based BYOL

Each Cloud Volumes ONTAP system that has a node-based BYOL must have a system license installed with an active subscription. Cloud Manager simplifies the process by managing licenses for you and by displaying a warning before they expire.

[Learn more about Cloud Volumes ONTAP licensing options.](#)

BYOL system licenses

A node-based license provides up to 368 TB of capacity for a single node or HA pair.

You can purchase multiple licenses for a Cloud Volumes ONTAP BYOL system to allocate more than 368 TB of capacity. For example, you might purchase two licenses to allocate up to 736 TB of capacity to Cloud Volumes ONTAP. Or you could purchase four licenses to get up to 1.4 PB.

The number of licenses that you can purchase for a single node system or HA pair is unlimited.



Some on-premises ONTAP storage systems that you purchased may have included a free Cloud Volumes ONTAP license. You can use the license to create a new Cloud Volumes ONTAP system, or you can apply the license to an existing Cloud Volumes ONTAP system to expand the capacity. [See if you have any available licenses to use.](#)

Be aware that disk limits can prevent you from reaching the capacity limit by using disks alone. You can go beyond the disk limit by [tiering inactive data to object storage](#). For information about disk limits, refer to [storage limits in the Cloud Volumes ONTAP Release Notes](#).

License management for a new system

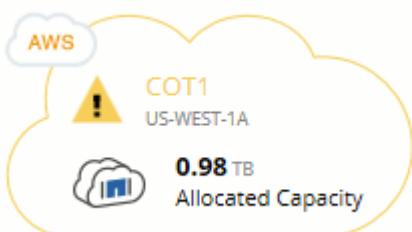
When you create a node-based BYOL system, Cloud Manager prompts you for the serial number of your license and your NetApp Support Site account. Cloud Manager uses the account to download the license file from NetApp and to install it on the Cloud Volumes ONTAP system.

[Learn how to add NetApp Support Site accounts to Cloud Manager.](#)

If Cloud Manager can't access the license file over the secure internet connection, you can [obtain the file yourself and then manually upload the file to Cloud Manager](#).

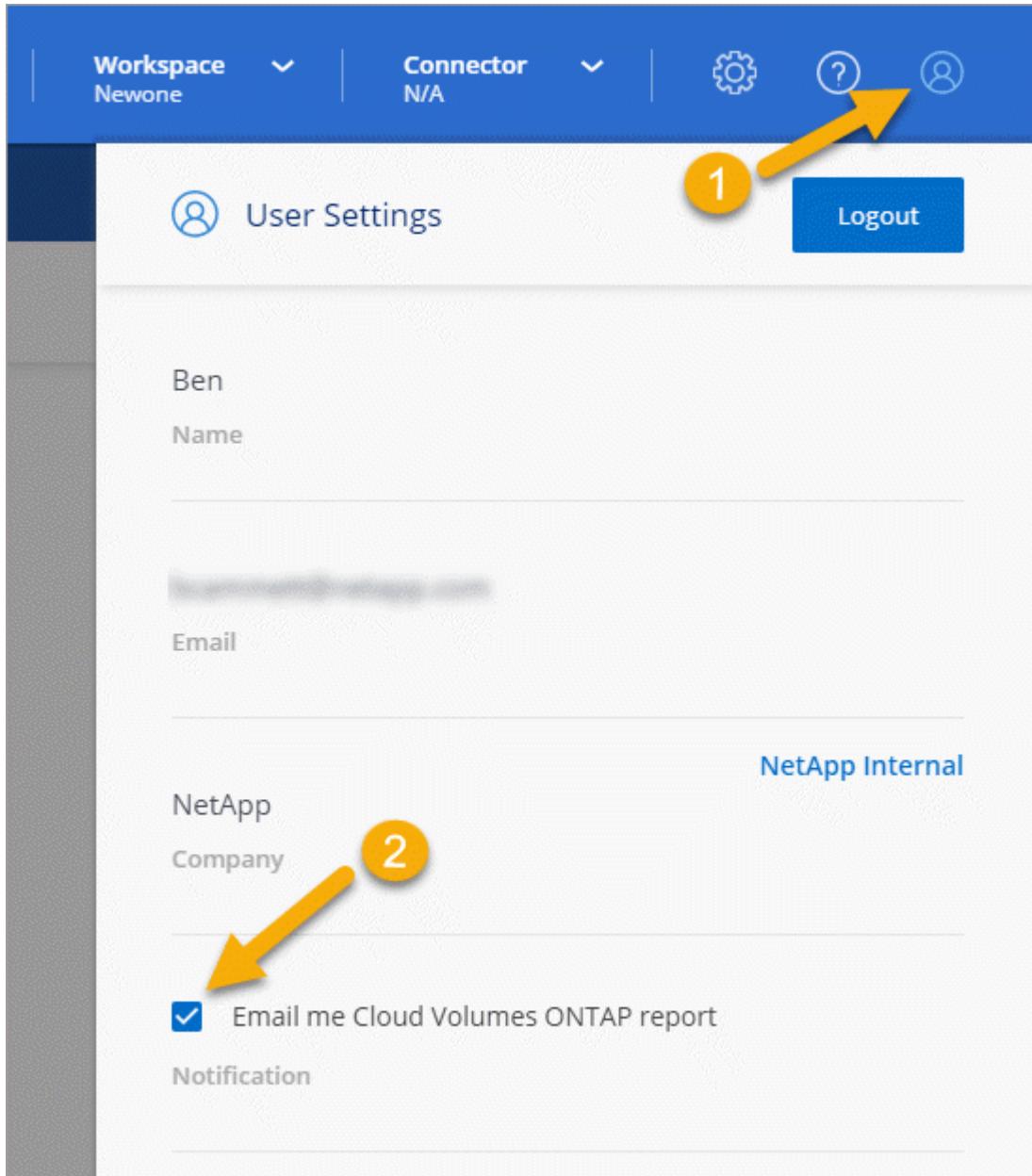
License expiration

Cloud Manager displays a warning 30 days before a node-based license is due to expire and again when the license expires. The following image shows a 30-day expiration warning that appears in the user interface:



You can select the working environment to review the message.

Cloud Manager includes a license expiration warning in the Cloud Volumes ONTAP report that's emailed to you, if you are an Account Admin and you enabled the option:



The emailed report includes the license expiration warning every 2 weeks.

If you don't renew the license in time, the Cloud Volumes ONTAP system shuts itself down. If you restart it, it shuts itself down again.

License renewal

When you renew a node-based BYOL subscription by contacting a NetApp representative, Cloud Manager automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system.

If Cloud Manager can't access the license file over the secure internet connection, you can [obtain the file yourself and then manually upload the file to Cloud Manager](#).

License transfer to a new system

A node-based BYOL license is transferable between Cloud Volumes ONTAP systems when you delete an existing system and then create a new one using the same license.

For example, you might want to delete an existing licensed system and then use the license with a new BYOL system in a different VPC/VNet or cloud provider. Note that only *cloud-agnostic* serial numbers work in any cloud provider. Cloud-agnostic serial numbers start with the 908xxxx prefix.

It's important to note that your BYOL license is tied to your company and a specific set of NetApp Support Site credentials.

Evaluating

You can evaluate Cloud Volumes ONTAP before you pay for the software. Three options are available: the Freemium offering, a 30-day free trial, and an evaluation license.

If you need assistance with your proof of concept, contact [the Sales team](#) or reach out through the chat option available from [NetApp Cloud Central](#) and from within Cloud Manager.

Freemium offering

The Freemium offering enables you to use all Cloud Volumes ONTAP features free of charge from NetApp (cloud provider charges still apply). You're limited to 500 GB of provisioned capacity per node and there's no support contract. You can have up to 10 Freemium systems.

[Learn more about the Freemium offering.](#)

30-day free trials for PAYGO

A 30-day free trial is available if you plan to pay for Cloud Volumes ONTAP as you go. You can start a 30-day free trial of Cloud Volumes ONTAP from Cloud Manager by creating your first Cloud Volumes ONTAP system in a payer's account.

There are no hourly software license charges for the instance, but infrastructure charges from your cloud provider still apply.

A free trial automatically converts to a paid hourly subscription when it expires. If you terminate the instance within the time limit, the next instance that you deploy is not part of the free trial (even if it's deployed within those 30 days).

Pay-as-you-go trials are awarded through a cloud provider and are not extendable by any means.

Evaluation license for node-based licensing

An evaluation BYOL license is an option for customers who expect to pay for Cloud Volumes ONTAP by purchasing a termed license from NetApp. You can obtain an evaluation license from your account team, your Sales Engineer, or your partner.

The evaluation key is good for 30 days, and can be used multiple times, each for 30 days (regardless of the creation day).

At the end of 30 days, daily shutdowns will occur, so it's best to plan ahead. You can apply a new BYOL license on top of the evaluation license for an in-place upgrade (this requires a restart of single node systems). Your hosted data is **not** deleted at the end of the trial period.



You can't upgrade Cloud Volumes ONTAP software when using an evaluation license.

Security

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

Encryption of data at rest

Cloud Volumes ONTAP supports the following encryption technologies:

- NetApp encryption solutions (NVE and NAE)
- AWS Key Management Service
- Azure Storage Service Encryption
- Google Cloud Platform default encryption

You can use NetApp encryption solutions with native encryption from AWS, Azure, or GCP, which encrypt data at the hypervisor level. Doing so would provide double encryption, which might be desired for very sensitive data. When the encrypted data is accessed, it's unencrypted twice—once at the hypervisor-level (using keys from the cloud provider) and then again using NetApp encryption solutions (using keys from an external key manager).

NetApp encryption solutions (NVE and NAE)

Cloud Volumes ONTAP supports both NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE) with an external key manager. NVE and NAE are software-based solutions that enable (FIPS) 140-2-compliant data-at-rest encryption of volumes.

- NVE encrypts data at rest one volume at a time. Each data volume has its own unique encryption key.
- NAE is an extension of NVE—it encrypts data for each volume, and the volumes share a key across the aggregate. NAE also allows common blocks across all volumes in the aggregate to be deduplicated.

Both NVE and NAE use AES 256-bit encryption.

[Learn more about NetApp Volume Encryption and NetApp Aggregate Encryption.](#)

Starting with Cloud Volumes ONTAP 9.7, new aggregates will have NetApp Aggregate Encryption (NAE) enabled by default after you set up an external key manager. New volumes that aren't part of an NAE aggregate will have NetApp Volume Encryption (NVE) enabled by default (for example, if you have existing aggregates that were created before setting up an external key manager).

Setting up a supported key manager is the only required step. For set up instructions, see [Encrypting volumes with NetApp encryption solutions](#).

AWS Key Management Service

When you launch a Cloud Volumes ONTAP system in AWS, you can enable data encryption using the [AWS Key Management Service \(KMS\)](#). Cloud Manager requests data keys using a customer master key (CMK).



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

If you want to use this encryption option, then you must ensure that the AWS KMS is set up appropriately. For details, see [Setting up the AWS KMS](#).

Azure Storage Service Encryption

[Azure Storage Service Encryption](#) for data at rest is enabled by default for Cloud Volumes ONTAP data in Azure. No setup is required.

You can encrypt Azure managed disks on single node Cloud Volumes ONTAP systems using external keys from another account. This feature is supported using Cloud Manager APIs.

You just need to add the following to the API request when creating the single node system:

```
"azureEncryptionParameters": {  
    "key": <azure id of encryptionset>  
}
```



Customer-managed keys are not supported with Cloud Volumes ONTAP HA pairs.

Google Cloud Platform default encryption

[Google Cloud Platform data-at-rest encryption](#) is enabled by default for Cloud Volumes ONTAP. No setup is required.

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

ONTAP virus scanning

You can use integrated antivirus functionality on ONTAP systems to protect data from being compromised by viruses or other malicious code.

ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

For information about the vendors, software, and versions supported by Vscan, see the [NetApp Interoperability Matrix](#).

For information about how to configure and manage the antivirus functionality on ONTAP systems, see the [ONTAP 9 Antivirus Configuration Guide](#).

Ransomware protection

Ransomware attacks can cost a business time, resources, and reputation. Cloud Manager enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

- Cloud Manager identifies volumes that are not protected by a Snapshot policy and enables you to activate the default Snapshot policy on those volumes.

Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the

granularity to create images of a single file copy or a complete disaster recovery solution.

- Cloud Manager also enables you to block common ransomware file extensions by enabling ONTAP's FPolicy solution.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection [i](#)

50 % Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes [i](#)

[Activate Snapshot Policy](#)

2 Block Ransomware File Extensions [i](#)

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names](#) [i](#)

[Activate FPolicy](#)

[Learn how to implement the NetApp solution for ransomware.](#)

Performance

You can review performance results to help you decide which workloads are appropriate for Cloud Volumes ONTAP.

- Cloud Volumes ONTAP for AWS

[NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads.](#)

- Cloud Volumes ONTAP for Microsoft Azure

[NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads.](#)

- Cloud Volumes ONTAP for Google Cloud

[NetApp Technical Report 4816: Performance Characterization of Cloud Volumes ONTAP for Google Cloud.](#)

AutoSupport and Active IQ Digital Advisor

The AutoSupport component of ONTAP collects telemetry and sends it for analysis. Active IQ Digital Advisor analyzes the data from AutoSupport and provides proactive care and optimization. Using artificial intelligence, Active IQ can identify potential problems and help you resolve them before they impact your business.

Active IQ enables you to optimize your data infrastructure across your global hybrid cloud by delivering actionable predictive analytics and proactive support through a cloud-based portal and mobile app. Data-driven insights and recommendations from Active IQ are available to all NetApp customers with an active

SupportEdge contract (features vary by product and support tier).

Here are some things you can do with Active IQ:

- Plan upgrades.

Active IQ identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP and the Upgrade Advisor component helps you plan for a successful upgrade.

- View system wellness.

Your Active IQ dashboard reports any issues with wellness and helps you correct those issues. Monitor system capacity to make sure you never run out of storage space. View support cases for your system.

- Manage performance.

Active IQ shows system performance over a longer period than you can see in ONTAP System Manager. Identify configuration and system issues that are impacting your performance. Maximize efficiency. View storage efficiency metrics and identify ways to store more data in less space.

- View inventory and configuration.

Active IQ displays complete inventory and software and hardware configuration information. See when service contracts are expiring and renew them to ensure you remain supported.

Related information

- [NetApp Documentation: Active IQ Digital Advisor](#)
- [Launch Active IQ](#)
- [SupportEdge Services](#)

Default configuration for Cloud Volumes ONTAP

Understanding how Cloud Volumes ONTAP is configured by default can help you set up and administer your systems, especially if you are familiar with ONTAP because the default setup for Cloud Volumes ONTAP is different than ONTAP.

Defaults

- Cloud Volumes ONTAP is available as a single-node system and as an HA pair in AWS, Azure, and GCP.
- Cloud Manager creates one data-serving storage VM when it deploys Cloud Volumes ONTAP. Some configurations support additional storage VMs. [Learn more about managing storage VMs](#).

Starting with the Cloud Manager 3.9.5 release, logical space reporting is enabled on the initial storage VM. When space is reported logically, ONTAP reports the volume space such that all the physical space saved by the storage efficiency features are also reported as used.

- Cloud Manager automatically installs the following ONTAP feature licenses on Cloud Volumes ONTAP:
 - CIFS
 - FlexCache
 - FlexClone

- iSCSI
- NetApp Volume Encryption (only for BYOL or registered PAYGO systems)
- NFS
- SnapMirror
- SnapRestore
- SnapVault
- Several network interfaces are created by default:
 - A cluster management LIF
 - An intercluster LIF
 - An SVM management LIF on HA systems in Azure and in GCP, on single node systems in AWS, and optionally on HA systems in multiple AWS Availability Zones
 - A node management LIF (in GCP, this LIF is combined with the intercluster LIF)
 - An iSCSI data LIF
 - A CIFS and NFS data LIF



LIF failover is disabled by default for Cloud Volumes ONTAP due to EC2 requirements. Migrating a LIF to a different port breaks the external mapping between IP addresses and network interfaces on the instance, making the LIF inaccessible.

- Cloud Volumes ONTAP sends configuration backups to the Connector using HTTPS.

The backups are accessible from <https://ipaddress/occm/offboxconfig/> where *ipaddress* is the IP address of the Connector host.

- Cloud Manager sets a few volume attributes differently than other management tools (System Manager or the CLI, for example).

The following table lists the volume attributes that Cloud Manager sets differently from the defaults:

Attribute	Value set by Cloud Manager
Autosize mode	grow
Maximum autosize	1,000 percent <div data-bbox="432 1510 489 1573" data-label="Image"> </div> The Account Admin can modify this value from the Settings page.
Security style	NTFS for CIFS volumes UNIX for NFS volumes
Space guarantee style	none
UNIX permissions (NFS only)	777

See the *volume create* man page for information about these attributes.

Internal disks for system data

In addition to the storage for user data, Cloud Manager also purchases cloud storage for system data.

AWS

- Two disks per node for boot and root data:
 - 9.7: 160 GB io1 disk for boot data and a 220 GB gp2 disk for root data
 - 9.6: 93 GB io1 disk for boot data and a 140 GB gp2 disk for root data
 - 9.5: 45 GB io1 disk for boot data and a 140 GB gp2 disk for root data
- Starting with version 9.8, a 540 GB General Purpose SSD (gp2) for a core disk when using a C5, M5, or R5 instance type
- One EBS snapshot for each boot disk and root disk
- For HA pairs, one EBS volume for the Mediator instance, which is approximately 8 GB

Azure (single node)

- Three Premium SSD disks:
 - One 10 GB disk for boot data
 - One 140 GB disk for root data
 - One 128 GB disk for NVRAM

If the virtual machine that you chose for Cloud Volumes ONTAP supports Ultra SSDs, then the system uses an Ultra SSD for NVRAM, rather than a Premium SSD.

- One 1024 GB Standard HDD disk for saving cores
- One Azure snapshot for each boot disk and root disk

Azure (HA pairs)

- Two 10 GB Premium SSD disks for the boot volume (one per node)
- Two 140 GB Premium Storage page blobs for the root volume (one per node)
- Two 1024 GB Standard HDD disks for saving cores (one per node)
- Two 128 GB Premium SSD disks for NVRAM (one per node)
- One Azure snapshot for each boot disk and root disk

GCP

- One 10 GB Standard persistent disk for boot data
- One 64 GB Standard persistent disk for root data
- One 500 GB Standard persistent disk for NVRAM
- One 315 GB Standard persistent disk for saving cores
- One GCP snapshot each for the boot disk and root disk

For an HA pair, there are two disks per node for root data.

Where the disks reside

Cloud Manager lays out the storage as follows:

- Boot data resides on a disk attached to the instance or virtual machine.

This disk, which contains the boot image, is not available to Cloud Volumes ONTAP.

- Root data, which contains the system configuration and logs, resides in aggr0.
- The storage virtual machine (SVM) root volume resides in aggr1.
- Data volumes also reside in aggr1.

Encryption

Boot and root disks are always encrypted in Azure and Google Cloud Platform because encryption is enabled by default in those cloud providers.

When you enable data encryption in AWS using the Key Management Service (KMS), the boot and root disks for Cloud Volumes ONTAP are encrypted, as well. This includes the boot disk for the mediator instance in an HA pair. The disks are encrypted using the CMK that you select when you create the working environment.

Get started in AWS

Getting started with Cloud Volumes ONTAP for AWS

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



Create a Connector

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



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.](#)



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.](#)



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](#).



Launch Cloud Volumes ONTAP using Cloud Manager

Click **Add Working Environment**, select the type of system that you would like to deploy, and complete the steps in the wizard. [Read step-by-step instructions](#).

Related links

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

Planning 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.

Viewing supported regions

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](#).

Choosing a license type

A few licensing options are available for Cloud Volumes ONTAP. Each of these licensing options enables you to choose a configuration that meets your needs.

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

Choosing a supported instance

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

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

Choosing a configuration that supports Flash Cache

Some Cloud Volumes ONTAP configurations in AWS include local NVMe storage, which Cloud Volumes ONTAP uses as *Flash Cache* for better performance. [Learn more about Flash Cache](#).

Understanding storage limits

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

[Storage limits for Cloud Volumes ONTAP 9.9.1 in AWS](#)

Sizing 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](#).

- *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.
- *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).

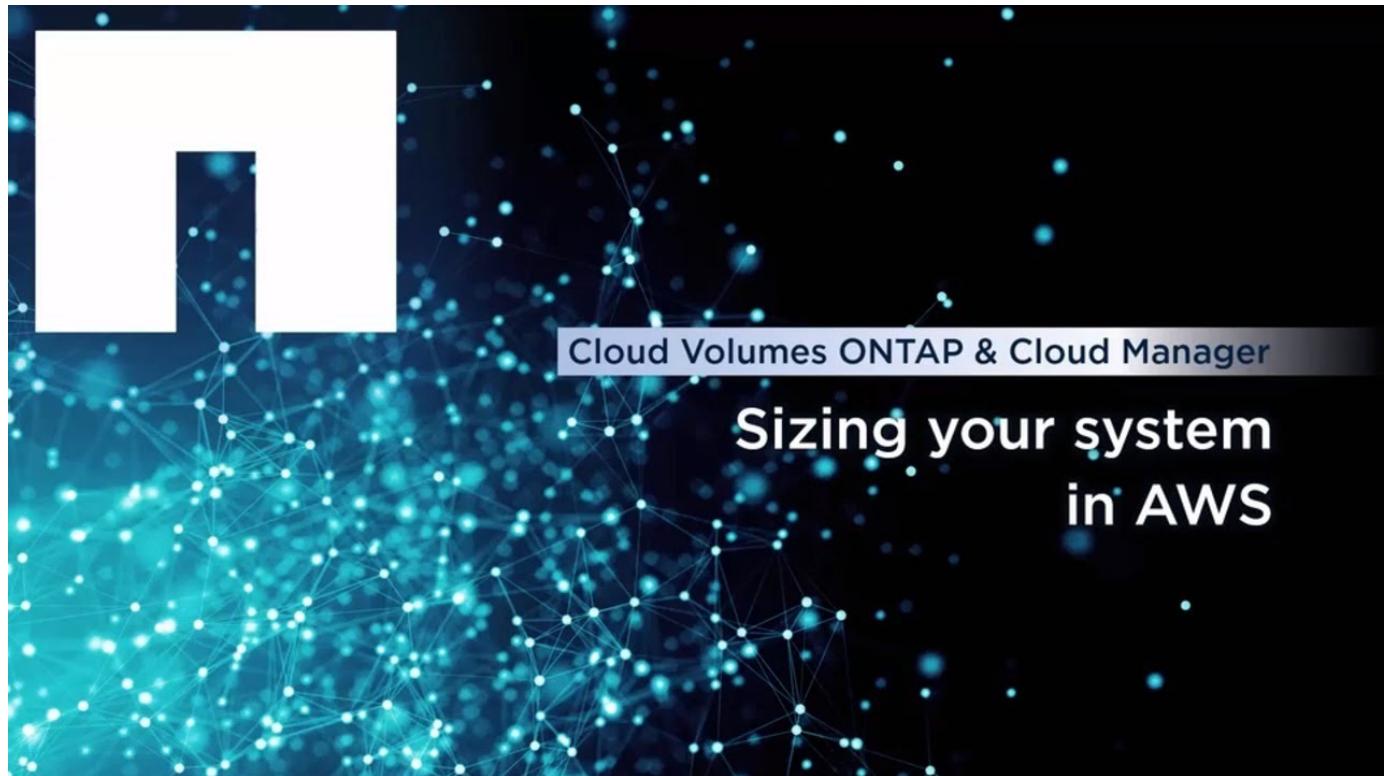
EBS disk size

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 [build 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 TB 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](#).

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



Preparing 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

AWS network information worksheet

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.

Network information for Cloud Volumes ONTAP

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

Network information for an 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	

AWS information	Your value
Floating IP address for data on node 1	
Floating IP address for data on node 2	
Route tables for floating IP addresses	

Choosing 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](#).

Choosing a volume usage profile

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

NetApp storage efficiency features provide the following benefits:

Thin provisioning

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

Deduplication

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

Compression

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

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 to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

Routing and firewall policies must allow AWS 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.

[Learn how to configure AutoSupport.](#)

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

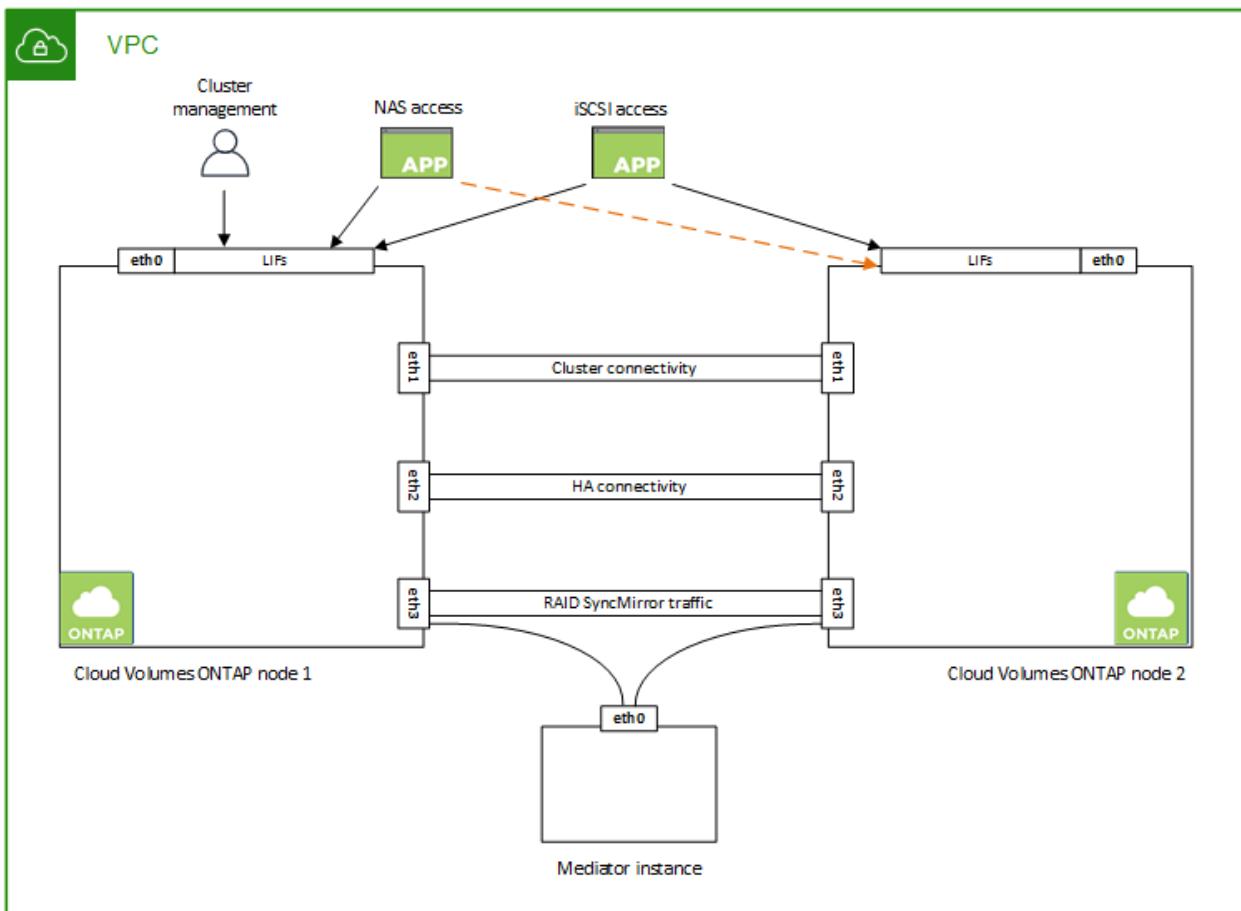
A storage VM management LIF is used with management tools like SnapCenter.

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:



AWS Cloud



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.
iSCSI data	eth0	node 1 and node 2	Client access over the iSCSI protocol.

LIF	Interface	Node	Purpose
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, an Azure VNet or 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](#).

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.



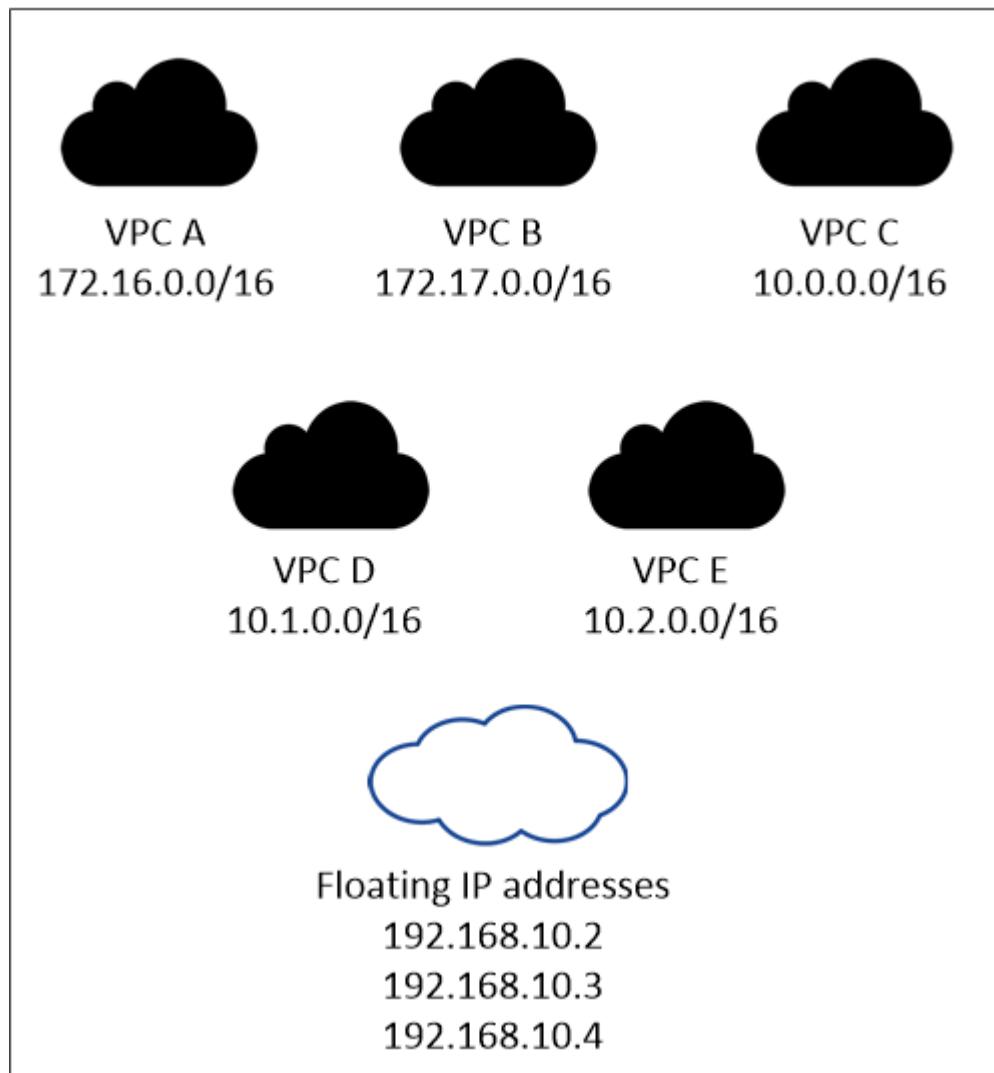
A floating IP address is required for the SVM management LIF if you use SnapDrive for Windows or SnapCenter with the HA pair. If you don't specify the IP address when you deploy the system, you can create the LIF later. For details, see [Setting up Cloud Volumes ONTAP](#).

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](#).

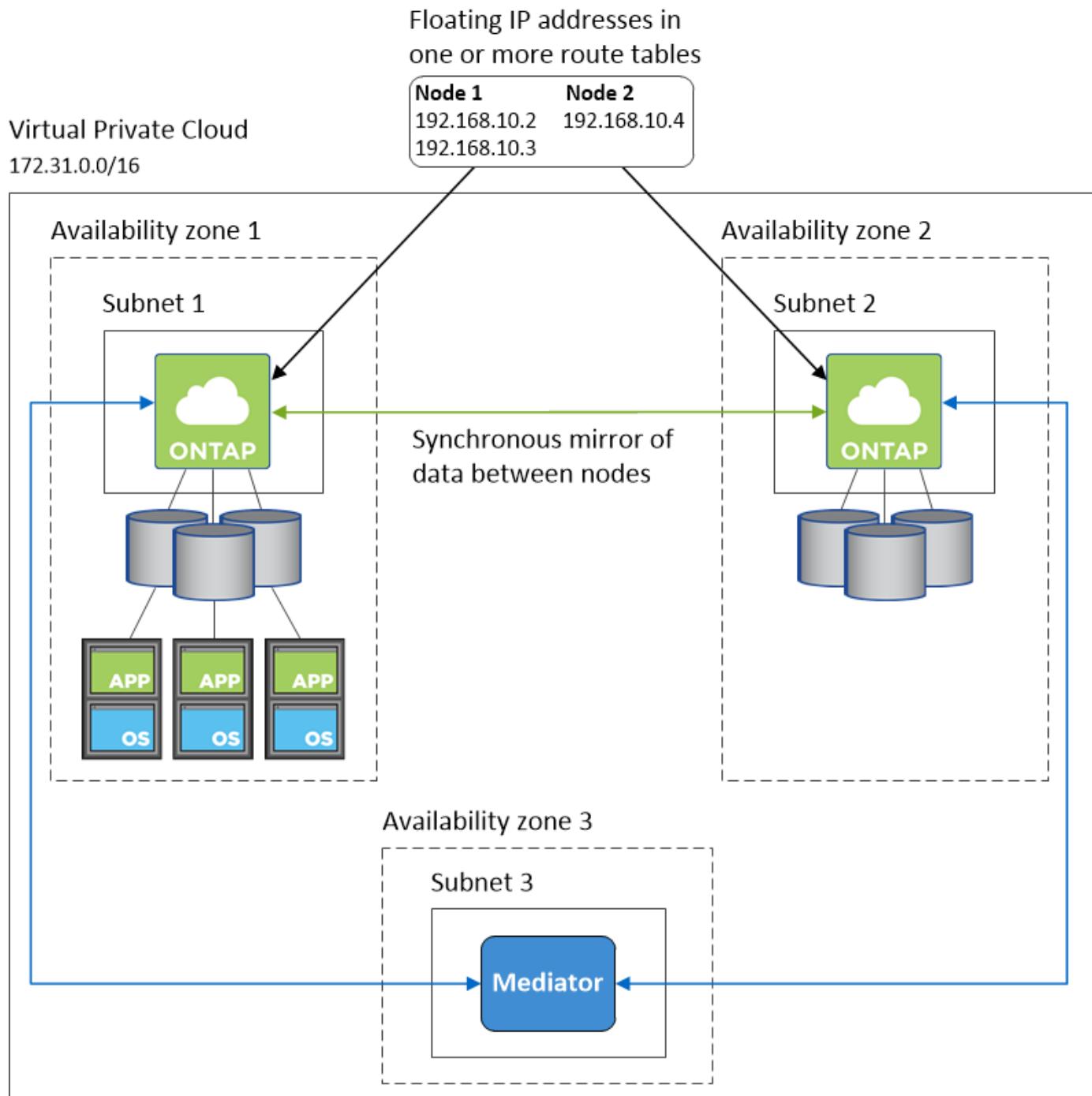
Connection to NetApp management tools

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. A Connector contacts the following endpoints when managing resources in AWS:



If your VPC uses a network access control list (ACL) to filter traffic, then make sure that you enable these endpoints for both outbound and inbound traffic.

Endpoints	Purpose
<p>AWS services (amazonaws.com):</p> <ul style="list-style-type: none">• CloudFormation• Elastic Compute Cloud (EC2)• Key Management Service (KMS)• Security Token Service (STS)• Simple Storage Service (S3) <p>The exact endpoint depends on the region in which you deploy Cloud Volumes ONTAP. Refer to AWS documentation for details.</p>	Enables the Connector to deploy and manage Cloud Volumes ONTAP in AWS.
https://api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
https://cloudmanagerinfraprod.azurecr.io *.blob.core.windows.net	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://cloudmanager.cloud.netapp.com	Communication with the Cloud Manager service, which includes Cloud Central accounts.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
support.netapp.com:443 https://mysupport.netapp.com	Communication with NetApp AutoSupport. Note that the Connector communicates with support.netapp.com:443, which redirects to https://mysupport.netapp.com.

Endpoints	Purpose
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication with NetApp for system licensing and support registration.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Enables NetApp to collect information needed to troubleshoot support issues.
https://ipa-signer.cloudmanager.netapp.com	Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)
Various third-party locations, for example: <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com <p>Third-party locations are subject to change.</p>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

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

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

Endpoints	Purpose
https://widget.intercom.io	For in-product chat that enables you to talk to NetApp cloud experts.

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

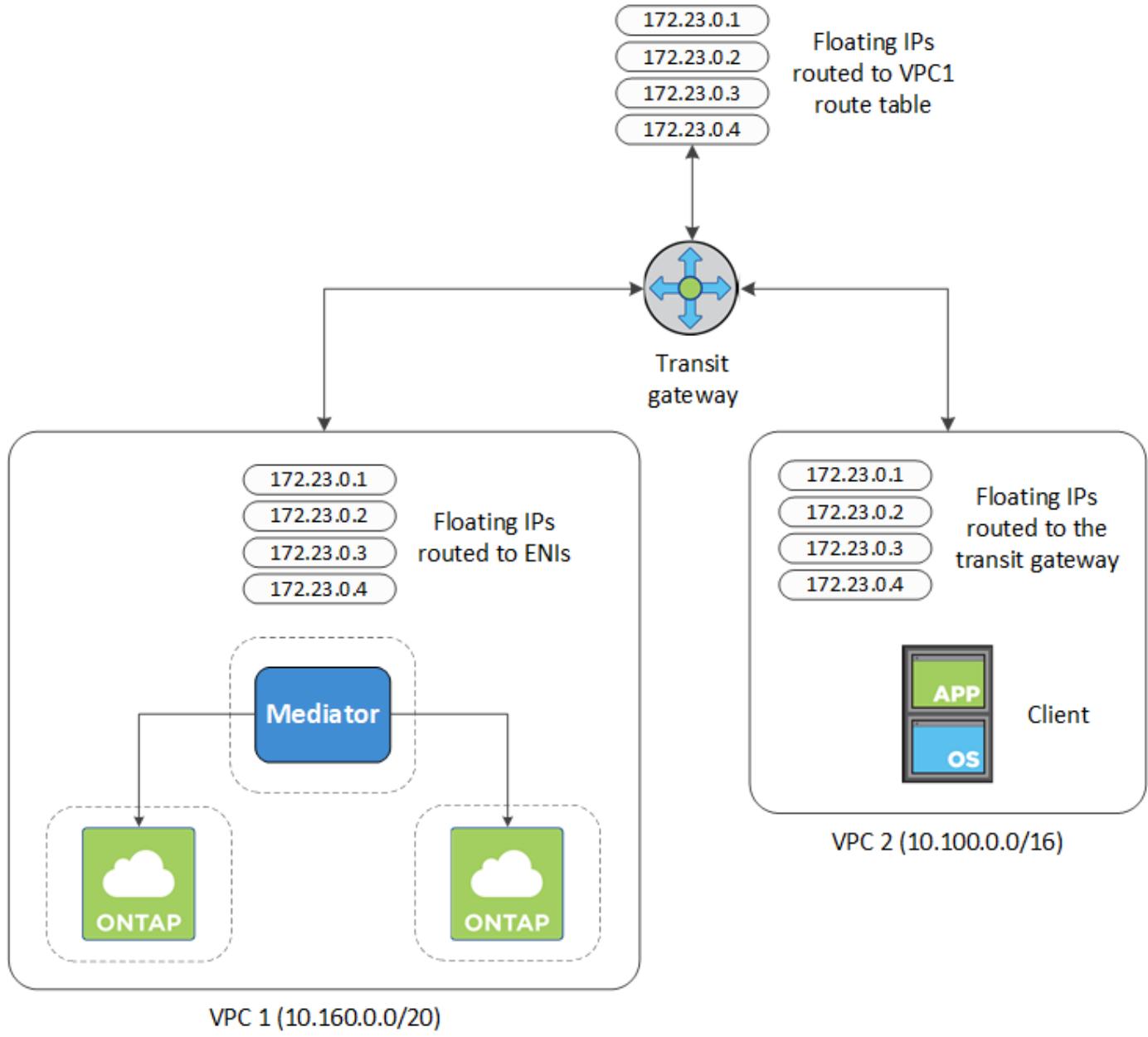
Set up an AWS transit gateway to enable access to an HA pair's [floating IP addresses](#) from outside the VPC where the HA pair resides.

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			
<input type="text"/> Filter by attributes or search by keyword					
CIDR	Attachment		Resource type	Route type	Route state
10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 vpc-0b2bc30e0dc8e0db1		VPC2	propagated	active
10.160.0.0/20	tgw-attach-00eba3eac3250d7db vpc-673ae603		VPC1	propagated	active
172.23.0.1/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active	
172.23.0.2/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active	
172.23.0.3/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active	
172.23.0.4/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active	

4. Modify the route table of VPCs that need to access the floating IP addresses.

- Add route entries to the floating IP addresses.
- 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	taw-015b7c249661ac279	active	No	VPC1
172.23.0.1/32	tgw-015b7c249661ac279	active	No	Floating IP Addresses
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	

5. 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.

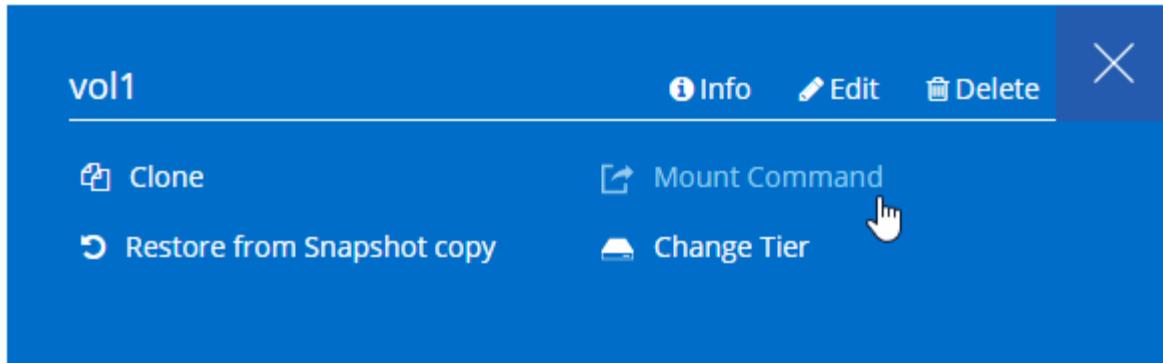
Route Table: rtb-0569a1bd740ed033f				
Summary	Routes	Subnet Associations	Route Propagation	Tags
Edit routes				
View All routes ▾				
Destination	Target	Status		
10.160.0.0/20	local	active		
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active		
0.0.0.0/0	igw-b2182dd7	active		
10.60.29.0/25	pcx-589c3331	active		
10.100.0.0/16	tgw-015b7c249661ac279	active		VPC2
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		

6. 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](#)

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 own security groups.

Rules for Cloud Volumes ONTAP

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

Inbound rules

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

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the System Manager web console using the IP address of the cluster management LIF
HTTPS	443	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF

Protocol	Port	Purpose
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
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)
Backup to S3	TCP	5010	Intercluster LIF	Backup endpoint or restore endpoint	Back up and restore operations for the Backup to S3 feature

Service	Protocol	Port	Source	Destination	Purpose
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
	TCP	3000	Node management LIF	HA mediator	ZAPI calls (Cloud Volumes ONTAP HA only)
	ICMP	1	Node management LIF	HA mediator	Keep alive (Cloud Volumes ONTAP HA only)
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860 0–18 699	Node management LIF	Destination servers	NDMP copy
SMTP	TCP	25	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	TCP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	TCP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
SnapMirr or	TCP	1110 4	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	1110 5	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
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 mediator internal security group

The predefined internal security group for the Cloud Volumes ONTAP HA mediator includes the following rules. 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 the Cloud Data Sense instance with internet access, if your AWS network doesn't use a NAT or proxy

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
All UDP	All	All outbound traffic

Advanced outbound rules

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



The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
Active Directory	TCP	88	Active Directory forest	Kerberos V authentication
	TCP	139	Active Directory forest	NetBIOS service session
	TCP	389	Active Directory forest	LDAP
	TCP	445	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	TCP	464	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	TCP	749	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	UDP	137	Active Directory forest	NetBIOS name service
	UDP	138	Active Directory forest	NetBIOS datagram service
	UDP	464	Active Directory forest	Kerberos key administration
API calls and AutoSupport	HTTP	443	Outbound internet and ONTAP cluster management LIF	API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp
API calls	TCP	3000	ONTAP cluster management LIF	API calls to ONTAP
	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](#)

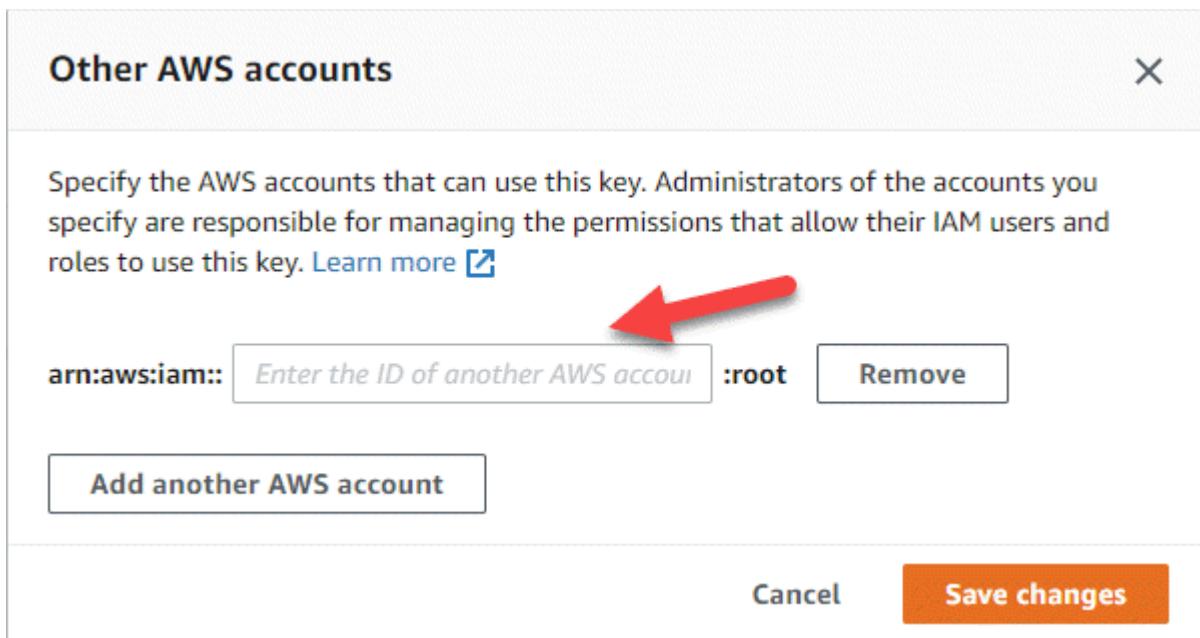
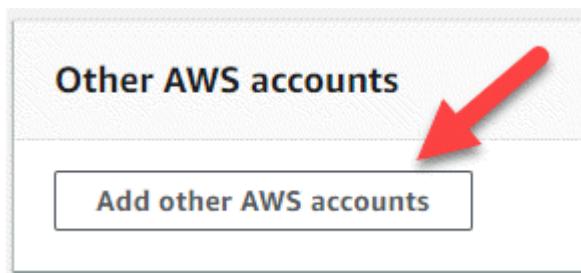
3. If the CMK is in a different AWS account, complete the following steps:

- Go to the KMS console from the account where the CMK resides.
- Select the key.
- 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.

- 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.



- Now switch to the AWS account that provides Cloud Manager with permissions and open the IAM console.
- Create an IAM policy that includes the permissions listed below.
- 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 External AWS Accounts to Access a CMK](#).

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](#)

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](#).

- DNS and Active Directory for CIFS configurations.

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

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

Licensing option	Requirement	How to meet the requirement
PAYGO free trial	A Marketplace subscription is required.	You'll have the option to subscribe to your cloud provider's marketplace from the Details & Credentials page.
Freemium	A Marketplace subscription or NetApp Support Site (NSS) account is required.	<p>You'll have the option to subscribe to your cloud provider's marketplace from the Details & Credentials page</p> <p>You can enter your NSS account on the Charging Methods and NSS Account page.</p>

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

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 admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.</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/occm//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](#).

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.

The following image shows the page filled out:

Location	Connectivity
AWS Region	Security Group
US West Oregon	<input checked="" type="radio"/> Generated security group <input type="radio"/> Use existing security group
VPC	SSH Authentication Method
vpc-3a01e05f - 172.31.0.0/16	<input checked="" type="radio"/> Password <input type="radio"/> Key Pair
Subnet	
172.31.5.0/24 (OCCM subnet)	

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

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 (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.

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, select a license, an instance type, and the instance tenancy.

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



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

13. **Underlying Storage Resources:** Choose settings for the initial aggregate: a disk type, a size for each disk, and whether data tiering 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 AWS](#).

- 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 Cloud Backup was enabled or if data tiering was enabled.

[Learn more about WORM storage.](#)

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

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

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

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

<p>Details & Protection</p> <p>Volume Name: <input type="text" value="vol"/> Size (GB): <input type="text" value="250"/></p> <p>Snapshot Policy: <input type="text" value="default"/></p> <p><small>i Default Policy</small></p>	<p>Protocol</p> <p>NFS CIFS iSCSI</p> <p>Share name: <input type="text" value="vol_share"/> Permissions: <input type="text" value="Full Control"/></p> <p>Users / Groups: <input type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>
---	--

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. 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.

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	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. 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. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources .
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.

Field	Description
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/occm//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. **Region & VPC:** Enter the network information that you recorded in the AWS worksheet.

The following image shows the page filled out for a multiple AZ configuration:

Region & VPC

AWS Region US East N. Virginia	VPC vpc-a76d91c2 - 172.31.0.0/16	Security group Use a generated security group
<div style="display: flex; justify-content: space-around;"> <div style="width: 33%;"> <p> Node 1:</p> <p>Availability Zone us-east-1a</p> <p>Subnet 172.31.8.0/24</p> </div> <div style="width: 33%;"> <p> Node 2:</p> <p>Availability Zone us-east-1b</p> <p>Subnet 172.31.9.0/24</p> </div> <div style="width: 33%;"> <p> Mediator:</p> <p>Availability Zone us-east-1c</p> <p>Subnet 172.31.2.0/24</p> </div> </div>		

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

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, select a license, an instance type, and the instance tenancy.

If your needs change after you launch the instances, you can modify the license or instance type later.



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

16. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type, a size for each disk, and whether data tiering 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 AWS](#).

- 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 Cloud Backup was enabled or if data tiering was enabled.

[Learn more about WORM storage](#).

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

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

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.
Initiator group and IQN (for iSCSI only)	<p>iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.</p> <p>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.</p> <p>iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs).</p> <p>When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, 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 <div style="margin-top: 10px;"> Volume Name: <input type="text" value="vol"/> Size (GB): <input type="text" value="250"/> </div> <div style="margin-top: 10px;"> Snapshot Policy: <input type="text" value="default"/> </div> <div style="margin-top: 10px;"> <small>Default Policy</small> </div>	Protocol <div style="margin-top: 10px;"> NFS CIFS iSCSI </div> <div style="margin-top: 10px;"> Share name: <input type="text" value="vol_share"/> Permissions: <input type="text" value="Full Control"/> </div> <div style="margin-top: 10px;"> Users / Groups: <input type="text" value="engineering"/> </div> <div style="margin-top: 10px; font-size: small;"> Valid users and groups separated by a semicolon </div>
--	--

19. **CIFS Setup:** If you selected 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. 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.

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.

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

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.

```
        "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>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": [
                "s3GetObject",
                "s3PutObject",
                "s3DeleteObject"
            ],
            "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

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

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
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

Protocol	Port	Purpose
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 Azure

Getting started with Cloud Volumes ONTAP for Azure

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



Create a Connector

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



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](#).



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

- [Evaluating](#)
- [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 Azure permissions](#)

Planning 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.

Choosing a license type

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

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

Supported VM types

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

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

Understanding storage limits

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

[Storage limits for Cloud Volumes ONTAP 9.9.1 in Azure](#)

Sizing 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 TB disks can provide better performance than 500 GB 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](#)

Choosing a configuration that supports Flash Cache

A Cloud Volumes ONTAP configuration in Azure includes local NVMe storage, which Cloud Volumes ONTAP uses as *Flash Cache* for better performance. [Learn more about Flash Cache](#).

Azure network information worksheet

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)	

Choosing 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](#).

Choosing a volume usage profile

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

NetApp storage efficiency features provide the following benefits:

Thin provisioning

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

Deduplication

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

Compression

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

Networking requirements for Cloud Volumes ONTAP in 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 for Cloud Volumes ONTAP

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

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

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

[Learn how to configure AutoSupport.](#)

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 the security group rules listed below.

Number of 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.

Connection from Cloud Volumes ONTAP to Azure Blob storage for data tiering

If you want to tier cold data to Azure Blob storage, you don't need to set up a connection between the performance tier and the capacity tier as long as Cloud Manager has the required permissions. Cloud Manager enables a VNet service endpoint for you if the Cloud Manager policy has these permissions:

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

These permissions are included in the latest [Cloud Manager policy](#).

For details about setting up data tiering, 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 Azure and ONTAP systems in other networks, you must have a VPN connection between the Azure VNet and the other network—for example, an AWS VPC or your corporate network.

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

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. A Connector contacts the following endpoints when managing resources in Azure:

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions.
https://management.microsoftazure.de https://login.microsoftonline.de	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure US Gov regions.
https://api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
https://cloudmanagerinfraprod.azurecr.io *.blob.core.windows.net	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://cloudmanager.cloud.netapp.com	Communication with the Cloud Manager service, which includes Cloud Central accounts.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
support.netapp.com:443 https://mysupport.netapp.com	Communication with NetApp AutoSupport. Note that the Connector communicates with support.netapp.com:443, which redirects to https://mysupport.netapp.com.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication with NetApp for system licensing and support registration.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Enables NetApp to collect information needed to troubleshoot support issues.
https://ipa-signer.cloudmanager.netapp.com	Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)
*.blob.core.windows.net	Required for HA pairs when using a proxy.

Endpoints	Purpose
<p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com <p>Third-party locations are subject to change.</p>	<p>During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.</p>

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

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

Security group rules for Cloud Volumes ONTAP

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

The rules listed below allow traffic, unless the description notes that it blocks specific inbound traffic.

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	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
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

Priority and name	Port and protocol	Source and destination	Description
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 AllowAzureLoad BalancerInBound	Any port Any protocol	AzureLoadBalanc er 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

The rules listed below allow traffic, unless the description notes that it blocks specific inbound traffic.



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	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

Priority and name	Port and protocol	Source and destination	Description
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
DHCP	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)
	68	UDP	Node management LIF	DHCP	DHCP client for first-time setup

Service	Port	Protocol	Source	Destination	Purpose
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

Security group rules for the Connector

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

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
Active Directory	88	TCP	Active Directory forest	Kerberos V authentication
	139	TCP	Active Directory forest	NetBIOS service session
	389	TCP	Active Directory forest	LDAP
	445	TCP	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	464	TCP	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	749	TCP	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	137	UDP	Active Directory forest	NetBIOS name service
	138	UDP	Active Directory forest	NetBIOS datagram service
	464	UDP	Active Directory forest	Kerberos key administration
API calls and AutoSupport	443	HTTP	Outbound internet and ONTAP cluster management LIF	API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp
API calls	3000	TCP	ONTAP cluster management LIF	API calls to ONTAP
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"
```

You can find the latest list of permissions on the [Cloud Manager policies page](#).

These 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.

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 in the Add Working Environment wizard for the licensing method that you want to use.

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

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>
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI.
Edit 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/occm//media/video_subscribing_azure.mp4 (video)

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 & Connectivity:** Select a location, a resource group, a security group, and then select the checkbox to confirm network connectivity between the Connector and the target location.

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

Field	Description
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.

Field	Description
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 style="display: flex; align-items: center;">  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>
Security group	<p>If you choose an existing security group, then it must meet Cloud Volumes ONTAP requirements. View the default security group.</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 these charging methods](#).
- [Learn what's required in the wizard for the licensing method that you want to use](#).

8. **Preconfigured Packages:** Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

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

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

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



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

10. **Subscribe from the Azure Marketplace:** Follow the steps if Cloud Manager could not enable programmatic deployments of Cloud Volumes ONTAP.

11. **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](#).

12. **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 Cloud Backup was enabled or if data tiering was enabled.

[Learn more about WORM storage](#).

13. **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](#).

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

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

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

Field	Description
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.
Initiator group and IQN (for iSCSI only)	<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):
<input type="text" value="vol"/>	<input type="text" value="250"/> i
Snapshot Policy:	
<input type="text" value="default"/> <div style="display: flex; justify-content: space-between; width: 100%;"> Default Policy i Default Policy </div>	

Protocol

NFS	CIFS	iSCSI								
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Share name:</td> <td style="width: 50%;">Permissions:</td> </tr> <tr> <td><input type="text" value="vol_share"/></td> <td> <input type="text" value="Full Control"/> <div style="display: flex; justify-content: space-between; width: 100%;"> Full Control ▼ </div> </td> </tr> <tr> <td colspan="2">Users / Groups:</td> </tr> <tr> <td colspan="2"><input type="text" value="engineering"/></td> </tr> </table>			Share name:	Permissions:	<input type="text" value="vol_share"/>	<input type="text" value="Full Control"/> <div style="display: flex; justify-content: space-between; width: 100%;"> Full Control ▼ </div>	Users / Groups:		<input type="text" value="engineering"/>	
Share name:	Permissions:									
<input type="text" value="vol_share"/>	<input type="text" value="Full Control"/> <div style="display: flex; justify-content: space-between; width: 100%;"> Full Control ▼ </div>									
Users / Groups:										
<input type="text" value="engineering"/>										
Valid users and groups separated by a semicolon										

15. 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>

Field	Description
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 Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter OU=AADDC Computers or OU=AADDC Users in this field.</p> <p>Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</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	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.

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

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

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

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

Get started in GCP

Getting started with Cloud Volumes ONTAP for Google Cloud

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



Create a Connector

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

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



Plan your configuration

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

[Learn more about planning your configuration.](#)



Set up your networking

- a. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
- b. If you plan to enable data tiering, [configure the Cloud Volumes ONTAP subnet for Private Google Access](#).
- c. If you're deploying an HA pair, ensure that you have four VPCs, each with their own subnet.
- d. If you're using a shared VPC, provide the *Compute Network User* role to the Connector service account.
- e. Enable outbound internet access from the target VPC so the Connector and Cloud Volumes ONTAP can contact several endpoints.

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

[Learn more about networking requirements.](#)



Set up a service account

Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable [data tiering](#) to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the [Cloud Backup Service](#) to back up volumes to low-cost object storage.

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

[Read step-by-step instructions.](#)

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

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

Planning your Cloud Volumes ONTAP configuration in Google Cloud

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

Choosing a license type

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

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

Supported machine types

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

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

Understanding storage limits

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

Storage limits for Cloud Volumes ONTAP 9.9.1 in GCP

Sizing your system in GCP

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

Machine type

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

Refer to the following for more details:

- [Google Cloud documentation: N1 standard machine types](#)
- [Google Cloud documentation: Performance](#)

GCP disk type

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

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

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

GCP disk size

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

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

Refer to the following for more details:

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

GCP network information worksheet

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

Network information for a single-node system

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

Network information for an HA pair in multiple zones

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

Network information for an HA pair in a single zone

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

Choosing a write speed

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

Choosing a volume usage profile

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

NetApp storage efficiency features provide the following benefits:

Thin provisioning

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

Deduplication

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

Compression

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

Networking requirements for Cloud Volumes ONTAP in GCP

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

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

Requirements for Cloud Volumes ONTAP

The following requirements must be met in GCP.

Internal load balancers

Cloud Manager automatically creates three Google Cloud internal load balancers (TCP/UDP) that manage incoming traffic to the Cloud Volumes ONTAP HA pair. (Prior to 9.9.0, four load balancers were created.) No setup is required from your end. We've listed this as a requirement simply to inform you of the network traffic and to mitigate any security concerns.

One load balancer is for cluster management, one is for NAS traffic to node 1, and the last is for NAS traffic to node 2.

The setup for each load balancer is as follows:

- One shared private IP address
- One global health check

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

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

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

One or multiple zones for HA pairs

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

- Multiple zones (recommended)

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

- Single zone

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

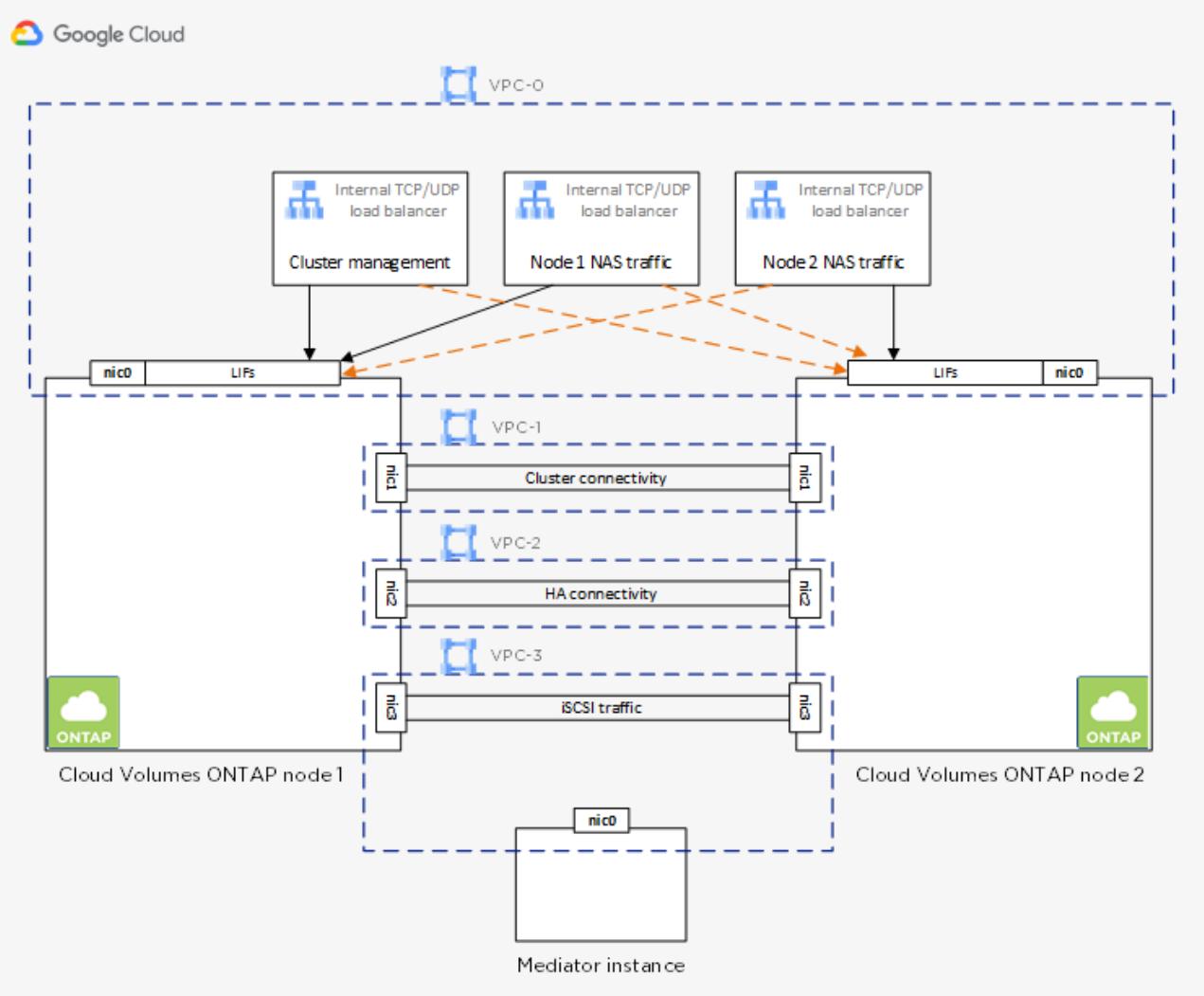
This deployment model does lower your costs because there are no data egress charges between zones.

Four Virtual Private Clouds for HA pairs

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

Cloud Manager will prompt you to choose four VPCs when you create the HA pair:

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



Subnets for HA pairs

A private subnet is required for each VPC.

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

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

One Virtual Private Cloud for single node systems

One VPC is required for a single node system.

Shared VPCs

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

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

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

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

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

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

Outbound internet access for Cloud Volumes ONTAP

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

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

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

[Learn how to configure AutoSupport](#).



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

Private IP addresses

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

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

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

```
skipSvmManagementLif: true
```

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

- **HA pair:** 15 or 16 private IP addresses

- 7 or 8 private IP addresses for VPC-0

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

```
skipSvmManagementLif: true
```

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

Firewall rules

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

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

- One set of rules for HA components in VPC-0. These rules enable data access to Cloud Volumes

ONTAP. [Learn more](#).

- Another set of rules for HA components in VPC-1, VPC-2, and VPC-3. These rules are open for inbound & outbound communication between the HA components. [Learn more](#).

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

If you want to tier cold data to a Google Cloud Storage bucket, the subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access (if you're using an HA pair, this is the subnet in VPC-0). For instructions, refer to [Google Cloud documentation: Configuring Private Google Access](#).

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

Connections to ONTAP systems in other networks

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

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

Requirements for the Connector

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



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

Connection to target networks

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

Outbound internet access

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

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

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

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

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

Firewall rules for Cloud Volumes ONTAP

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

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

If you're deploying an HA configuration, these are the firewall rules for Cloud Volumes ONTAP in VPC-0.

Inbound rules

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

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

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the System Manager web console using the IP address of the cluster management LIF
HTTPS	443	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF

Protocol	Port	Purpose
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
TCP	63001-63050	Load balance probe ports to determine which node is healthy (required for HA pairs only)
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
UDP	635	NFS mount
UDP	2049	NFS server daemon
UDP	4045	NFS lock daemon
UDP	4046	Network status monitor for NFS
UDP	4049	NFS rquotad protocol

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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



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

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

Service	Protocol	Port	Source	Destination	Purpose
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
	TCP	3000	Node management LIF	HA mediator	ZAPI calls (Cloud Volumes ONTAP HA only)
	ICMP	1	Node management LIF	HA mediator	Keep alive (Cloud Volumes ONTAP HA only)
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860 0–18 699	Node management LIF	Destination servers	NDMP copy
SMTP	TCP	25	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	TCP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	TCP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
SnapMirr or	TCP	1110 4	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	1110 5	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
Syslog	UDP	514	Node management LIF	Syslog server	Syslog forward messages

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

In GCP, an HA configuration is deployed across four VPCs. The firewall rules needed for the HA configuration in VPC-0 are [listed above for Cloud Volumes ONTAP](#).

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

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

Firewall rules for the Connector

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

Inbound rules

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

Outbound rules

The predefined firewall rules for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

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

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

Advanced outbound rules

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



The source IP address is the Connector host.

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

Create a service account for data tiering and backups

Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable [data tiering](#) to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the [Cloud Backup Service](#) to back up volumes to low-cost object storage.

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

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

Steps

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

Create service account

Service account details

2 Grant this service account access to project (optional)

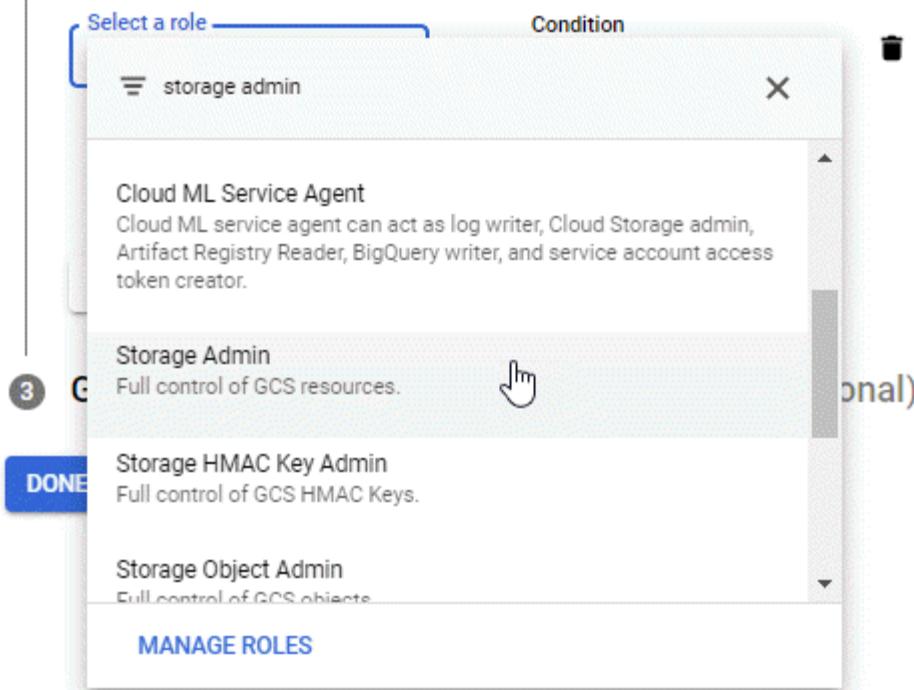
Grant this service account access to OCCM-Dev so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Select a role Condition

Role	Description	Condition
storage admin	Cloud ML Service Agent Cloud ML service agent can act as log writer, Cloud Storage admin, Artifact Registry Reader, BigQuery writer, and service account access token creator.	
Storage Admin	Storage Admin Full control of GCS resources.	
Storage HMAC Key Admin	Storage HMAC Key Admin Full control of GCS HMAC Keys.	
Storage Object Admin	Storage Object Admin Full control of GCS objects.	

DONE

[MANAGE ROLES](#)



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

This step is required for data tiering only. It's not required for the Cloud Backup Service.

Create service account

Service account details

Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

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

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com 



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

Service account admins role



Grant users the permission to administer this service account

DONE

CANCEL

What's next?

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

Details and Credentials

default-project Google Cloud Project	gcp-sub2 Marketplace Subscription	Edit Project
<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>Details</p> <p>Working Environment Name (Cluster Name)</p> <input type="text" value="cloudvolumesontap"/> </div> <div style="width: 45%;"> <p>Credentials</p> <p>User Name</p> <input type="text" value="admin"/> </div> </div>		
<div style="margin-top: 10px;"> <div style="display: flex; align-items: center;"> Service Account <small>i</small> <input checked="" type="checkbox"/> </div> <div style="margin-top: 10px;"> <p>Service Account Name</p> <input type="text" value="account1"/> </div> <div style="margin-top: 10px;"> + Add Labels <small>Optional Field Up to four labels</small> </div> </div>		
<p>Password</p> <input type="password"/> <p>Confirm Password</p> <input type="password"/>		

Using customer-managed encryption keys with Cloud Volumes ONTAP

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

Steps

1. Ensure that the Cloud Manager Connector service account has the correct permissions in the project where the key is stored.

The permissions are provided by the [Cloud Manager YAML file](#) by default, but may not be applied if you use an alternate project for the Cloud Key Management Service.

The permissions are as follows:

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

2. Ensure that the service account for the [Google Compute Engine Service Agent](#) has Cloud KMS Encrypter/Decrypter on the key.

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

3. Obtain the "id" of the key by invoking the get command for the [/gcp/vsa/metadata/gcp-encryption-keys](#) API call or by choosing "Copy Resource Name" on the key in the GCP console.
4. Use the "GcpEncryption" parameter with your API request when creating a working environment.

Example

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

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

Launching Cloud Volumes ONTAP in GCP

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

Before you get started

You need the following to create a working environment.

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

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

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

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

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

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

Launching a single-node system in GCP

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

Steps

- On the Canvas page, click **Add Working Environment** and follow the prompts.
- Choose a Location:** Select **Google Cloud** and **Cloud Volumes ONTAP**.
- If you're prompted, [create a Connector](#).
- Details & Credentials:** Select a project, specify a cluster name, optionally select a Service Account, optionally add labels, and then specify credentials.

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

Field	Description
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the GCP VM instance. It also uses the name as the prefix for the predefined security group, if you select that option.

Field	Description
Service Account Name	If you plan to use 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 admin account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI.
Edit Project	<p>Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where Cloud Manager resides.</p> <p>If you don't see any additional projects in the drop-down list, then you haven't yet associated the Cloud Manager service account with other projects. Go to the Google Cloud console, open the IAM service, and select the project. Add the service account with the Cloud Manager role to that project. You'll need to repeat this step for each project.</p> <p> This is the service account that you set up for Cloud Manager, as described on this page.</p> <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:

► https://docs.netapp.com/us-en/occm//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 select the checkbox to confirm network connectivity to Google Cloud storage for data tiering.

If you want to tier cold data to a Google Cloud Storage bucket, the subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access. For instructions, refer to [Google Cloud Documentation: Configuring Private Google Access](#).

7. **Charging Methods and NSS Account:** Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.
 - [Learn about these charging methods.](#)
 - [Learn what's required in the wizard for the licensing method that you want to use.](#)

8. **Preconfigured Packages:** Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

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

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

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



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

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

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

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

For help choosing a disk type and size, see [Sizing your system in GCP](#).

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

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

[Learn more about write speed.](#)

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

[Learn more about WORM storage.](#)

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

Note the following:

- Cloud Manager sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Connector

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

- For help with adding a GCP account, see [Setting up and adding GCP accounts for data tiering with 9.6](#).
- You can choose a specific volume tiering policy when you create or edit a volume.
- If you disable data tiering, you can enable it on subsequent aggregates, but you'll need to turn off the system and add a service account from the GCP console.

[Learn more about data tiering](#).

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

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

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.
Initiator group and IQN (for iSCSI only)	iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs. iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs). 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 .

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

The screenshot shows the 'Volume Details, Protection & Protocol' page. In the 'Protocol' section, 'CIFS' is selected. Under 'Details & Protection', the 'Volume Name' is 'vol' and the 'Size (GB)' is '250'. The 'Snapshot Policy' is set to 'default'. A note indicates 'Default Policy'. In the 'Protocol' section, the 'Share name' is 'vol_share' and the 'Permissions' are 'Full Control'. The 'Users / Groups' field contains 'engineering'. A note states 'Valid users and groups separated by a semicolon'.

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

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select 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.

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>

Field	Description
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI.
Edit Project	<p>Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where Cloud Manager resides.</p> <p>If you don't see any additional projects in the drop-down list, then you haven't yet associated the Cloud Manager service account with other projects. Go to the Google Cloud console, open the IAM service, and select the project. Add the service account with the Cloud Manager role to that project. You'll need to repeat this step for each project.</p> <p> This is the service account that you set up for Cloud Manager, as described in step 4b on this page.</p> <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:

► https://docs.netapp.com/us-en/occm//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.](#)

7. **Charging Methods and NSS Account:** Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.

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

8. **Preconfigured Packages:** Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

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

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

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



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

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

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

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

For help choosing a disk type and size, see [Sizing your system in GCP](#).

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

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

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

Note the following:

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

[Learn more about data tiering](#).

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

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

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.

Field	Description
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.
Initiator group and IQN (for iSCSI only)	<p>iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.</p> <p>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.</p> <p>iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host 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 <div style="margin-top: 10px;"> Volume Name: <input type="text" value="vol"/> Size (GB): <input type="text" value="250"/> </div> <div style="margin-top: 10px;"> Snapshot Policy: <input type="text" value="default"/> </div> <div style="margin-top: 10px;"> <small>Default Policy</small> </div>	Protocol <div style="margin-top: 10px;"> <input checked="" type="radio"/> NFS <input checked="" type="radio"/> CIFS <input type="radio"/> iSCSI </div> <div style="margin-top: 10px;"> Share name: <input type="text" value="vol_share"/> Permissions: <input type="text" value="Full Control"/> </div> <div style="margin-top: 10px;"> Users / Groups: <input type="text" value="engineering"/> <div style="font-size: small; margin-top: -10px;">Valid users and groups separated by a semicolon</div> </div>
--	--

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

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select 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.

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

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

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

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

Result

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

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

For additional help, go to [NetApp Cloud Volumes ONTAP Support](#).

After you finish

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

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

Planning for VPC Service Controls in GCP

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

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

How NetApp services communicate with VPC Service Controls

NetApp services such as Cloud Central and Cloud Manager communicate directly with the Google Cloud APIs. This is either triggered from an external IP address outside of Google Cloud (for example, from `api.services.cloud.netapp.com`), or within Google Cloud from an internal address assigned to the Cloud Manager Connector.

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

Images

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

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

Deploying a Connector

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

Deploying Cloud Volumes ONTAP

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

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

VPC Service Controls perimeter policies

Policies allow exceptions to the VPC Service Controls rule sets. For more information about policies, please visit the [GCP VPC Service Controls Policy Documentation](#).

To set the policies that Cloud Manager requires, navigate to your VPC Service Controls Perimeter within your

organization and add the following policies. The fields should match the options given in the VPC Service Controls policy page. Also note that **all** rules are required and the **OR** parameters should be used in the rule set.

Ingress rules

Rule 1

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

OR

Rule 2

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

OR

Rule 3

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

Egress rules

Rule 1:

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



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

Provision and manage storage

Provisioning storage

You can provision additional storage for your Cloud Volumes ONTAP systems from Cloud Manager by managing volumes and aggregates.



All disks and aggregates must be created and deleted directly from Cloud Manager. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

Creating FlexVol volumes

If you need more storage after you launch your initial Cloud Volumes ONTAP system, you can create new

FlexVol volumes for NFS, CIFS, or iSCSI from Cloud Manager.

A Cloud Manager feature called "templates" enables you to create volumes that are optimized for the workload requirements for certain applications; such as databases or streaming services. If your organization has created volume templates that you should use, follow [these steps](#).

About this task

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](#).



You can create additional LUNs from System Manager or the CLI.

Before you begin

If you want to use CIFS in AWS, you must have set up DNS and Active Directory. For details, see [Networking requirements for Cloud Volumes ONTAP for AWS](#).

Steps

1. On the Canvas page, double-click the name of the Cloud Volumes ONTAP system on which you want to provision FlexVol volumes.
2. Create a new volume on any aggregate or on a specific aggregate:

Action	Steps
Create a new volume and let Cloud Manager choose the containing aggregate	Click Add Volume > New volume .
Create a new volume on a specific aggregate	<ol style="list-style-type: none">a. Click the menu icon, and then click Advanced > Advanced allocation.b. Click the menu for an aggregate.c. Click Create volume.

3. Enter details for the new volume, and then click **Continue**.

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>

4. If you chose the CIFS protocol and the CIFS server has not been set up, specify details for the server in the Create a CIFS Server dialog box, and then click **Save and continue**:

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	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <ul style="list-style-type: none"> To configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter OU=Computers,OU=corp in this field. To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter OU=AADDC Computers or OU=AADDC Users in this field. <p>Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</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	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.

- On the Usage Profile, Disk Type, and Tiering Policy page, choose whether you want to enable storage efficiency features, choose a disk type, and edit the tiering policy, if needed.

For help, refer to the following:

- [Understanding volume usage profiles](#)
- [Sizing your system in AWS](#)
- [Sizing your system in Azure](#)
- [Sizing your system in GCP](#)
- [Data tiering overview](#)

- Click **Go**.

Result

Cloud Volumes ONTAP provisions the volume.

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, you must 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.

Creating volumes from templates

If your organization has created Cloud Volumes ONTAP volume templates so you can deploy volumes that are optimized for the workload requirements for certain applications, follow the steps in this section.

The template should make your job easier because certain volume parameters will already be defined in the template, such as disk type, size, protocol, snapshot policy, cloud provider, and more. When a parameter is

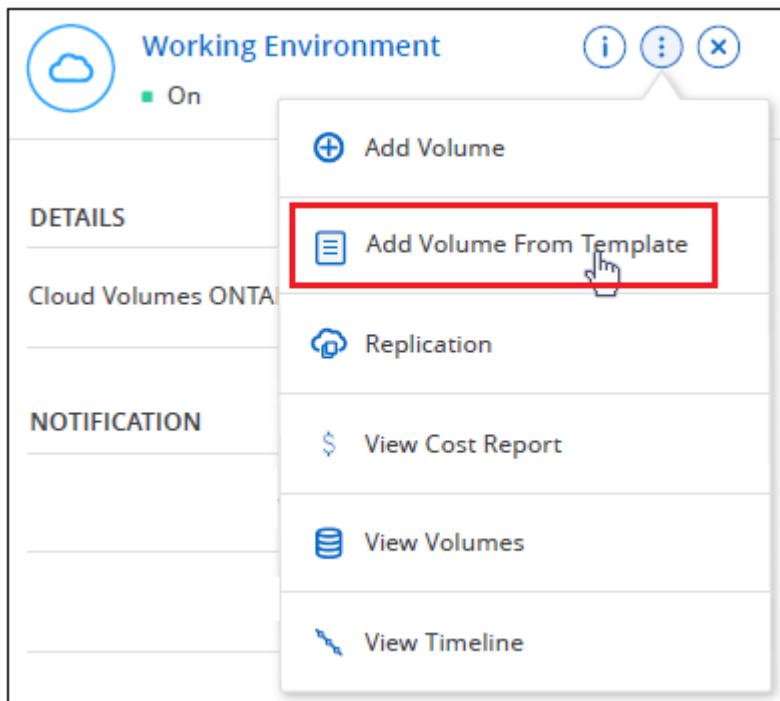
already predefined, you can just skip to the next volume parameter.



You can only create NFS or CIFS volumes when using templates.

Steps

1. On the Canvas page, click the name of the Cloud Volumes ONTAP system on which you want to provision a volume.
2. Click > **Add Volume From Template**.



3. In the *Select Template* page, select the template that you want to use to create the volume and click **Next**.

The screenshot shows the 'Select Template' page. At the top, there are two tabs: '1 Select Template' and '2 Define Parameters'. Below the tabs, the title 'Select Template' is displayed. A search bar is on the right. The main area shows a table with two rows of data. The first row, 'AWS CVO volume for production', has a checked checkbox in the first column and is highlighted with a red box. The second row, 'AWS CVO volume for staging', is also present. The columns are labeled 'Template Name', 'Template Description', 'Created by', 'Last Modified', and 'Parameters'.

	Template Name	Template Description	Created by	Last Modified	Parameters
<input checked="" type="checkbox"/>	AWS CVO volume for production	High efficiency with daily backup	Rabin	Apr 05 2021, 1:39:30 pm	View
	AWS CVO volume for staging	High efficiency with weekly backup	Rabin	Apr 05 2021, 1:34:20 pm	View

The *Define Parameters* page is displayed.

Define Parameters

Enter your values for the actions. Parameters that are locked by the template are not editable.

Actions

```

graph TD
    A[Create Volume in Cloud Volumes  
ONTAP (1)] --> B[Enable Cloud Backup (1)]
    
```

Show read-only parameters

Details ⓘ

Volume Name	Volume Name should start with "staging"
Volume Size (GB)	Minimum value is 160, Maximum value is 185

Protection ⓘ

Snapshot Policy	Default
-----------------	---------

Usage Profile ⓘ

<input checked="" type="radio"/> Storage Efficiency	<input type="radio"/> No Storage Efficiency
---	---

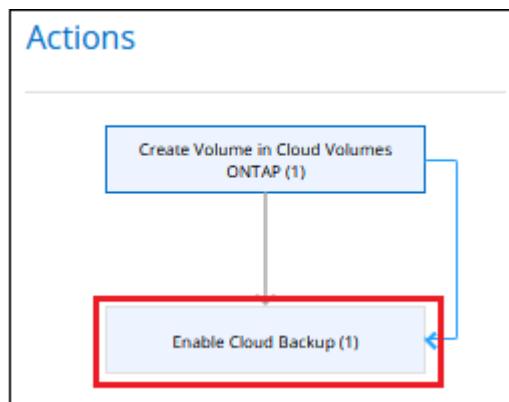
Disk Type

Disk Type	GP2 - General Purpose SSD
-----------	---------------------------

Note: You can click the checkbox **Show read-only parameters** to show all the fields that have been locked by the template if you want to see the values for those parameters. By default these predefined fields are hidden and only the fields you need to complete are shown.

4. In the **Context** area, the Working Environment is filled in with the name of the working environment you started with. You need to select the **Storage VM** where the volume will be created.
5. Add values for all of the parameters that are not hard-coded from the template. See [creating volumes](#) for details about all the parameters you need to complete to deploy a Cloud Volumes ONTAP volume.
6. If there are no other Actions that you need to define (for example, configuring Cloud Backup), click **Run Template**.

If there are other actions, click the action in the left pane to display the parameters you need to complete.

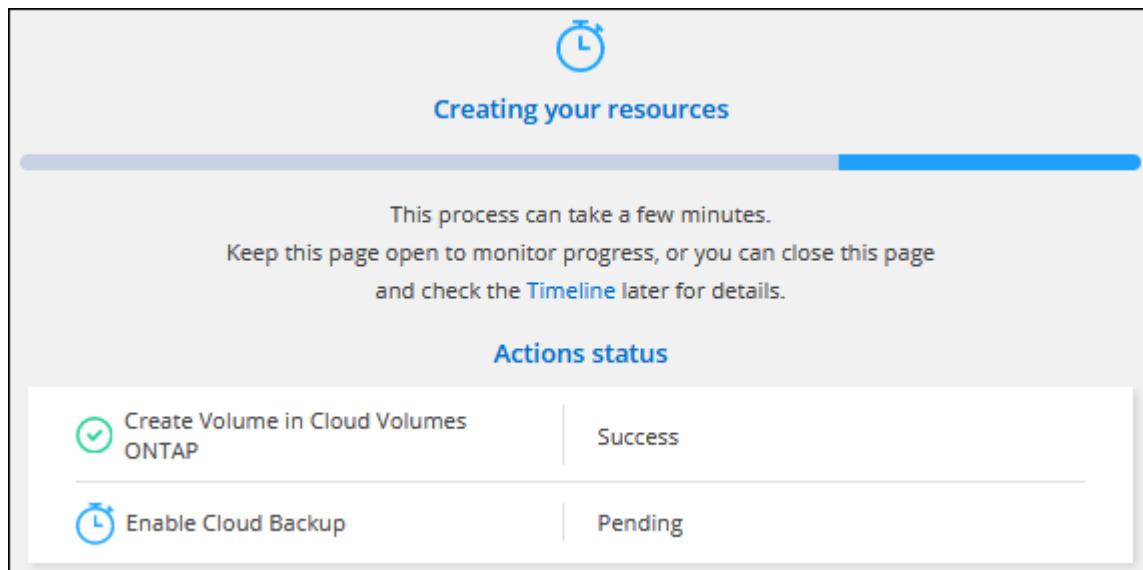


For example, if the Enable Cloud Backup action requires that you select a backup policy, you can do that now.

7. Click **Run Template**.

Result

Cloud Volumes ONTAP provisions the volume and displays a page so that you can see the progress.



Additionally, if any secondary action is implemented in the template, for example, enabling Cloud Backup on the volume, that action is also performed.

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, you must 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.

Creating FlexVol volumes on the second node in an HA configuration

By default, Cloud Manager creates volumes on the first node in an HA configuration. If you need an active-active configuration, in which both nodes serve data to clients, you must create aggregates and volumes on the second node.

Steps

1. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
2. Click the menu icon and then click **Advanced > Advanced allocation**.
3. Click **Add Aggregate** and then create the aggregate.
4. For Home Node, choose the second node in the HA pair.
5. After Cloud Manager creates the aggregate, select it and then click **Create volume**.
6. Enter details for the new volume, and then click **Create**.

After you finish

You can create additional volumes on this aggregate if required.



For HA pairs deployed in multiple AWS Availability Zones, you must mount the volume to clients by using the floating IP address of the node on which the volume resides.

Creating aggregates

You can create aggregates yourself or let Cloud Manager do it for you when it creates volumes. The benefit of creating aggregates yourself is that you can choose the underlying disk size, which enables you to size your aggregate for the capacity or the performance that you need.

Steps

1. On the Canvas page, double-click the name of the Cloud Volumes ONTAP instance on which you want to manage aggregates.
2. Click the menu icon, and then click **Advanced > Advanced allocation**.
3. Click **Add Aggregate** and then specify details for the aggregate.

For help with disk type and disk size, see [Planning your configuration](#).

4. Click **Go**, and then click **Approve and Purchase**.

Connecting a LUN to a host

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.

Note the following:

1. Cloud Manager's automatic capacity management doesn't apply to LUNs. When Cloud Manager creates a LUN, it disables the autogrow feature.
2. You can create additional LUNs from System Manager or the CLI.

Steps

1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.
2. Select a volume, and then click **Target IQN**.
3. Click **Copy** to copy the IQN name.
4. Set up an iSCSI connection from the host to the LUN.
 - [ONTAP 9 iSCSI express configuration for Red Hat Enterprise Linux: Starting the iSCSI sessions with the target](#)
 - [ONTAP 9 iSCSI express configuration for Windows: Starting iSCSI sessions with the target](#)

Using FlexCache volumes to accelerate data access

A FlexCache volume is a storage volume that caches NFS read data from an origin (or source) volume. Subsequent reads to the cached data result in faster access to that data.

You can use FlexCache volumes to speed up access to data or to offload traffic from heavily accessed volumes. FlexCache volumes help improve performance, especially when clients need to access the same data repeatedly, because the data can be served directly without having to access the origin volume. FlexCache volumes work well for system workloads that are read-intensive.

Cloud Manager does not provide management of FlexCache volumes at this time, but you can use the ONTAP CLI or ONTAP System Manager to create and manage FlexCache volumes:

- [FlexCache Volumes for Faster Data Access Power Guide](#)
- [Creating FlexCache volumes in System Manager](#)

Starting with the 3.7.2 release, Cloud Manager generates a FlexCache license for all new Cloud Volumes ONTAP systems. The license includes a 500 GB usage limit.



To generate the license, Cloud Manager needs to access <https://ipa-signer.cloudmanager.netapp.com>. Make sure that this URL is accessible from your firewall.



Managing existing storage

Cloud Manager enables you to manage volumes, aggregates, and CIFS servers. It also prompts you to move volumes to avoid capacity issues.

Managing existing volumes

You can manage existing volumes as your storage needs change. You can view, edit, clone, restore, and delete volumes.

Steps

1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.
2. Manage your volumes:

Task	Action
View information about a volume	Select a volume, and then click Info .

Task	Action
Edit a volume (read-write volumes only)	<p>a. Select a volume, and then click Edit.</p> <p>b. Modify the volume's Snapshot policy, NFS protocol version, NFS access control list (export policy), or share permissions, and then click Update.</p> <p> If you need custom Snapshot policies, you can create them by using System Manager.</p>
Clone a volume	<p>a. Select a volume, and then click Clone.</p> <p>b. Modify the clone name as needed, and then click Clone.</p> <p>This process creates a FlexClone volume. A FlexClone volume is a writable, point-in-time copy that is space-efficient because it uses a small amount of space for metadata, and then only consumes additional space as data is changed or added.</p> <p>To learn more about FlexClone volumes, see the ONTAP 9 Logical Storage Management Guide.</p>
Restore data from a Snapshot copy to a new volume	<p>a. Select a volume, and then click Restore from Snapshot copy.</p> <p>b. Select a Snapshot copy, enter a name for the new volume, and then click Restore.</p>
Create a Snapshot copy on demand	<p>a. Select a volume, and then click Create a Snapshot copy.</p> <p>b. Change the name, if needed, and then click Create.</p>
Get the NFS mount command	<p>a. Select a volume, and then click Mount Command.</p> <p>b. Click Copy.</p>
View the target iQN for an iSCSI volume	<p>a. Select a volume, and then click Target iQN.</p> <p>b. Click Copy.</p> <p>c. Use the IQN to connect to the LUN from your hosts.</p>
Change the underlying disk type	<p>a. Select a volume, and then click Change Disk Type & Tiering Policy.</p> <p>b. Select the disk type, and then click Change.</p> <p> Cloud Manager moves the volume to an existing aggregate that uses the selected disk type or it creates a new aggregate for the volume.</p>

Task	Action
Change the tiering policy	<p>a. Select a volume, and then click Change Disk Type & Tiering Policy. b. Click Edit Policy. c. Select a different policy and click Change.</p> <div style="display: flex; align-items: center;"> i <p>Cloud Manager moves the volume to an existing aggregate that uses the selected disk type with tiering, or it creates a new aggregate for the volume.</p> </div>
Delete a volume	<p>a. Select a volume, and then click Delete. b. Click Delete again to confirm.</p>

Resizing a volume

By default, a volume automatically grows to a maximum size when it's out of space. The default value is 1,000, which means the volume can grow to 11 times its size. This value is configurable in a Connector's settings.

If you need to resize your volume, you can do it through [ONTAP System Manager](#). Be sure to take your system's capacity limits into consideration as you resize volumes. Go to the [Cloud Volumes ONTAP Release Notes](#) for more details.

Managing existing aggregates

Manage aggregates yourself by adding disks, viewing information about the aggregates, and by deleting them.

Before you begin

If you want to delete an aggregate, you must have first deleted the volumes in the aggregate.

About this task

If an aggregate is running out of space, you can move volumes to another aggregate by using OnCommand System Manager.

Steps

1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
2. Click the menu icon and then click **Advanced > Advanced allocation**.
3. Manage your aggregates:

Task	Action
View information about an aggregate	Select an aggregate and click Info .
Create a volume on a specific aggregate	Select an aggregate and click Create volume .

Task	Action
Add disks to an aggregate	<p>a. Select an aggregate and click Add AWS disks or Add Azure disks.</p> <p>b. Select the number of disks that you want to add and click Add.</p> <div style="display: flex; align-items: center;">  All disks in an aggregate must be the same size. </div>
Delete an aggregate	<p>a. Select an aggregate that does not contain any volumes and click Delete.</p> <p>b. Click Delete again to confirm.</p>

Modifying the CIFS server

If you change your DNS servers or Active Directory domain, you need to modify the CIFS server in Cloud Volumes ONTAP so that it can continue to serve storage to clients.

Steps

1. From the working environment, click the menu icon and then click **Advanced > CIFS setup**.
2. Specify settings for the CIFS server:

Task	Action
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.
Organizational Unit	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <p>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.</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	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.

3. Click **Save**.

Result

Cloud Volumes ONTAP updates the CIFS server with the changes.

Moving a volume

Move volumes for capacity utilization, improved performance, and to satisfy service-level agreements.

You can move a volume in System Manager by selecting a volume and the destination aggregate, starting the volume move operation, and optionally monitoring the volume move job. When using System Manager, a volume move operation finishes automatically.

Steps

1. Use System Manager or the CLI to move the volumes to the aggregate.

In most situations, you can use System Manager to move volumes.

For instructions, see the [ONTAP 9 Volume Move Express Guide](#).

Moving a volume when Cloud Manager displays an Action Required message

Cloud Manager might display an Action Required message that says moving a volume is necessary to avoid capacity issues, but that it cannot provide recommendations to correct the issue. If this happens, you need to identify how to correct the issue and then move one or more volumes.

Steps

1. [Identify how to correct the issue](#).
2. Based on your analysis, move volumes to avoid capacity issues:
 - [Move volumes to another system](#).
 - [Move volumes to another aggregate on the same system](#).

Identifying how to correct capacity issues

If Cloud Manager cannot provide recommendations for moving a volume to avoid capacity issues, you must identify the volumes that you need to move and whether you should move them to another aggregate on the same system or to another system.

Steps

1. View the advanced information in the Action Required message to identify the aggregate that has reached its capacity limit.

For example, the advanced information should say something similar to the following: Aggregate aggr1 has reached its capacity limit.

2. Identify one or more volumes to move out of the aggregate:

- a. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
- b. Select the aggregate, and then click **Info**.
- c. Expand the list of volumes.

Used Aggregate Capacity: 105.66 GB

Volumes:

4

Vol54 (54 GB)

data_vol (150 GB)

svm_FinanceOnPrem_root (1 GB)



- d. Review the size of each volume and choose one or more volumes to move out of the aggregate.

You should choose volumes that are large enough to free space in the aggregate so that you avoid additional capacity issues in the future.

3. If the system has not reached the disk limit, you should move the volumes to an existing aggregate or a new aggregate on the same system.

For details, see [Moving volumes to another aggregate to avoid capacity issues](#).

4. If the system has reached the disk limit, do any of the following:

- a. Delete any unused volumes.
- b. Rearrange volumes to free space on an aggregate.

For details, see [Moving volumes to another aggregate to avoid capacity issues](#).

- c. Move two or more volumes to another system that has space.

For details, see [Moving volumes to another system to avoid capacity issues](#).

Moving volumes to another system to avoid capacity issues

You can move one or more volumes to another Cloud Volumes ONTAP system to avoid capacity issues. You might need to do this if the system reached its disk limit.

About this task

You can follow the steps in this task to correct the following Action Required message:

Moving a volume is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you because the system has reached the disk limit.

Steps

1. Identify a Cloud Volumes ONTAP system that has available capacity, or deploy a new system.
2. Drag and drop the source working environment on the target working environment to perform a one-time data replication of the volume.

For details, see [Replicating data between systems](#).

3. Go to the Replication Status page, and then break the SnapMirror relationship to convert the replicated volume from a data protection volume to a read/write volume.

For details, see [Managing data replication schedules and relationships](#).

4. Configure the volume for data access.

For information about configuring a destination volume for data access, see the [ONTAP 9 Volume Disaster Recovery Express Guide](#).

5. Delete the original volume.

For details, see [Managing existing volumes](#).

Moving volumes to another aggregate to avoid capacity issues

You can move one or more volumes to another aggregate to avoid capacity issues.

About this task

You can follow the steps in this task to correct the following Action Required message:

Moving two or more volumes is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you.

Steps

1. Verify whether an existing aggregate has available capacity for the volumes that you need to move:
 - a. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
 - b. Select each aggregate, click **Info**, and then view the available capacity (aggregate capacity minus used aggregate capacity).

aggr1

Aggregate Capacity: 442.94 GB

Used Aggregate Capacity: 105.66 GB

2. If needed, add disks to an existing aggregate:
 - a. Select the aggregate, and then click **Add disks**.
 - b. Select the number of disks to add, and then click **Add**.
3. If no aggregates have available capacity, create a new aggregate.

For details, see [Creating aggregates](#).

4. Use System Manager or the CLI to move the volumes to the aggregate.

5. In most situations, you can use System Manager to move volumes.

For instructions, see the [ONTAP 9 Volume Move Express Guide](#).

Reasons why a volume move might perform slowly

Moving a volume might take longer than you expect if any of the following conditions are true for Cloud Volumes ONTAP:

- The volume is a clone.
- The volume is a parent of a clone.
- The source or destination aggregate has a single Throughput Optimized HDD (st1) disk.
- The Cloud Volumes ONTAP system is in AWS and one aggregate uses an older naming scheme for objects. Both aggregates have to use the same name format.

An older naming scheme is used if data tiering was enabled on an aggregate in the 9.4 release or earlier.

- The encryption settings don't match on the source and destination aggregates, or a rekey is in progress.
- The *-tiering-policy* option was specified on the volume move to change the tiering policy.
- The *-generate-destination-key* option was specified on the volume move.

Tiering inactive data to low-cost object storage

You can reduce storage costs for Cloud Volumes ONTAP by combining an SSD or HDD performance tier for hot data with an object storage capacity tier for inactive data. Data tiering is powered by FabricPool technology. For a high-level overview, see [Data tiering overview](#).

To set up data tiering, you need to do the following:



Choose a supported configuration

Most configurations are supported. If you have a Cloud Volumes ONTAP Standard, Premium, or BYOL system running the most recent version, then you should be good to go. [Learn more](#).



Ensure connectivity between Cloud Volumes ONTAP and object storage

- For AWS, you'll need a VPC Endpoint to S3. [Learn more](#).
- For Azure, you won't need to do anything as long as Cloud Manager has the required permissions. [Learn more](#).
- For GCP, you need to configure the subnet for Private Google Access and set up a service account. [Learn more](#).

3

Ensure that you have an aggregate with tiering enabled

Data tiering must be enabled on an aggregate in order to enable data tiering on a volume. You should be aware of the requirements for new volumes and for existing volumes. [Learn more](#).

4

Choose a tiering policy when creating, modifying, or replicating a volume

Cloud Manager prompts you to choose a tiering policy when you create, modify, or replicate a volume.

- [Tiering data on read-write volumes](#)
- [Tiering data on data protection volumes](#)

What's not required for data tiering?

- You don't need to install a feature license to enable data tiering.
- You don't need to create the capacity tier (an S3 bucket, Azure Blob container, or GCP bucket). Cloud Manager does that for you.
- You don't need to enable data tiering at the system level.



Cloud Manager creates an object store for cold data when the system is created, [as long as there are no connectivity or permissions issues](#). After that, you just need to enable data tiering on volumes (and in some cases, [on aggregates](#)).

Configurations that support data tiering

You can enable data tiering when using specific configurations and features:

- Data tiering is supported with Cloud Volumes ONTAP Standard, Premium, and BYOL, starting with the following versions:
 - Version 9.2 in AWS
 - Version 9.4 in Azure with single node systems
 - Version 9.6 in Azure with HA pairs
 - Version 9.6 in GCP



Data tiering is not supported in Azure with the DS3_v2 virtual machine type.

- In AWS, the performance tier can be General Purpose SSDs (gp3 or gp2) or Provisioned IOPS SSDs (io1).



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

- In Azure, the performance tier can be Premium SSD managed disks, Standard SSD managed disks, or Standard HDD managed disks.
- In GCP, the performance tier can be either SSDs or HDDs (standard disks).
- Data tiering is supported with encryption technologies.

- Thin provisioning must be enabled on volumes.

Requirements

Depending on your cloud provider, certain connections and permissions must be set up so that Cloud Volumes ONTAP can tier cold data to object storage.

Requirements to tier cold data to AWS S3

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?](#)

Requirements to tier cold data to Azure Blob storage

You don't need to set up a connection between the performance tier and the capacity tier as long as Cloud Manager has the required permissions. Cloud Manager enables a VNet service endpoint for you if the Cloud Manager policy has these permissions:

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

The permissions are included in the latest [Cloud Manager policy](#).

Requirements 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](#).
- You need a service account that meets the following requirements:
 - It must have the predefined Storage Admin role.
 - The Connector service account must be a *Service Account User* of this tiering service account.

[Read step-by-step instructions.](#)

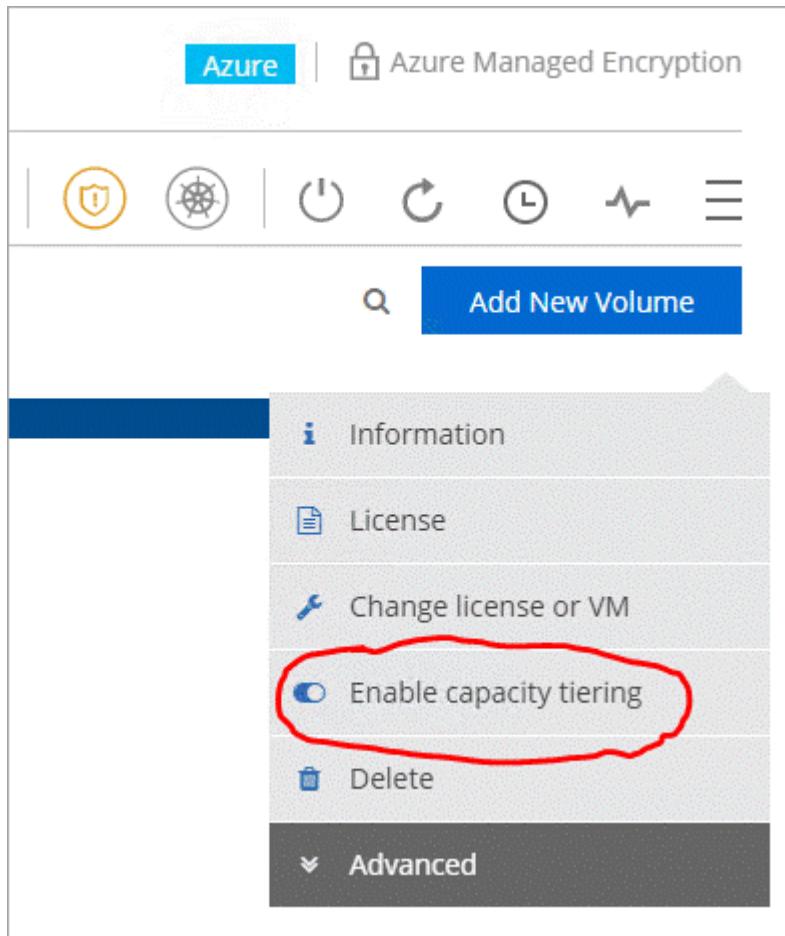
Enabling data tiering after implementing the requirements

Cloud Manager creates an object store for cold data when the system is created, as long as there are no connectivity or permissions issues. If you didn't implement the requirements listed above until after you created the system, then you'll need to manually enable tiering, which creates the object store.

Steps

1. [Ensure that you've met all requirements.](#)
2. On the Canvas page, double-click the name of the Cloud Volumes ONTAP instance.

3. Click the menu icon and select **Enable capacity tiering**.



You'll only see this option if data tiering couldn't be enabled when Cloud Manager created the system.

4. Click **Enable** so Cloud Manager can create the object store that this Cloud Volumes ONTAP system will use for tiered data.

Ensuring that tiering is enabled on aggregates

Data tiering must be enabled on an aggregate in order to enable data tiering on a volume. You should be aware of the requirements for new volumes and for existing volumes.

- **New volumes**

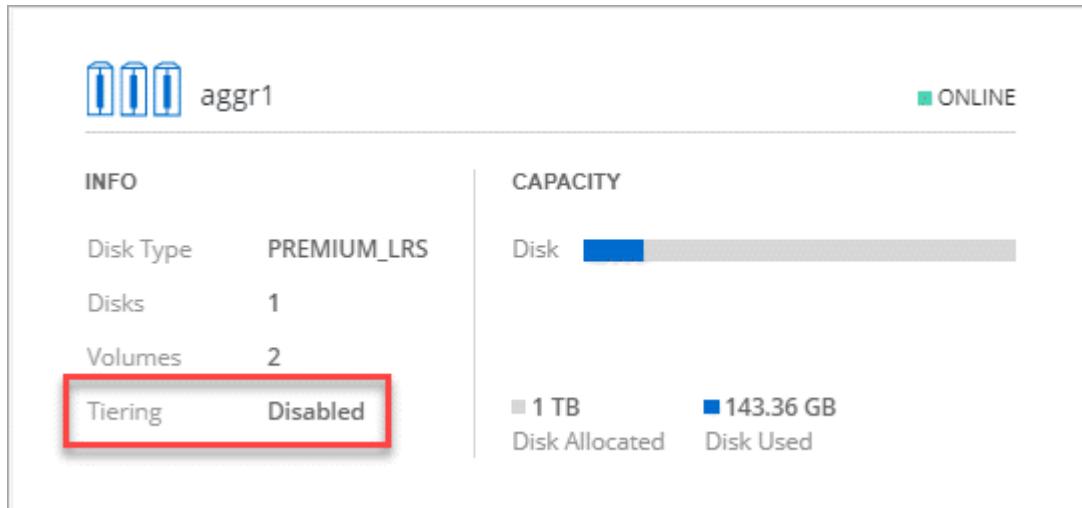
If you're enabling data tiering on a new volume, then you don't need to worry about enabling data tiering on an aggregate. Cloud Manager creates the volume on an existing aggregate that has tiering enabled, or it creates a new aggregate for the volume if a data tiering-enabled aggregate doesn't already exist.

- **Existing volumes**

If you want to enable data tiering on an existing volume, then you'll need to ensure that data tiering is enabled on the underlying aggregate. If data tiering isn't enabled on the existing aggregate, then you'll need to use System Manager to attach an existing aggregate to the object store.

Steps to confirm whether tiering is enabled on an aggregate

1. Open the working environment in Cloud Manager.
2. Click the menu icon, click **Advanced**, and then click **Advanced allocation**.
3. Verify whether tiering is enabled or disabled on the aggregate.



Steps to enable tiering on an aggregate

1. In System Manager, click **Storage > Tiers**.
2. Click the action menu for the aggregate and select **Attach Cloud Tiers**.
3. Select the cloud tier to attach and click **Save**.

What's next?

You can now enable data tiering on new and existing volumes, as explained in the next section.

Tiering data from read-write volumes

Cloud Volumes ONTAP can tier inactive data on read-write volumes to cost-effective object storage, freeing up the performance tier for hot data.

Steps

1. In the working environment, create a new volume or change the tier of an existing volume:

Task	Action
Create a new volume	Click Add New Volume .
Modify an existing volume	Select the volume and click Change Disk Type & Tiering Policy .

2. Select a tiering policy.

For a description of these policies, see [Data tiering overview](#).

Example



Tiering data to object storage

i Volume Tiering Policy

- All - Immediately tiers all data (not including metadata) to object storage.
- Auto - Tiers cold Snapshot copies and cold user data from the active file system to object storage.
- Snapshot Only - Tiers cold Snapshot copies to object storage
- None - Data tiering is disabled.

i Working Environment S3 Storage classes: Standard

Cloud Manager creates a new aggregate for the volume if a data tiering-enabled aggregate does not already exist.

Tiering data from data protection volumes

Cloud Volumes ONTAP can tier data from a data protection volume to a capacity tier. If you activate the destination volume, the data gradually moves to the performance tier as it is read.

Steps

1. On the Canvas page, select the working environment that contains the source volume, and then drag it to the working environment to which you want to replicate the volume.
2. Follow the prompts until you reach the tiering page and enable data tiering to object storage.

Example



S3 Tiering

i What are storage tiers?

- Enabled
- Disabled

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

For help with replicating data, see [Replicating data to and from the cloud](#).

Changing the storage class for tiered data

After you deploy Cloud Volumes ONTAP, you can reduce your storage costs by changing the storage class for inactive data that hasn't been accessed for 30 days. The access costs are higher if you do access the data, so you must take that into consideration before you change the storage class.

The storage class for tiered data is system wide—it's not per volume.

For information about supported storage classes, see [Data tiering overview](#).

Steps

1. From the working environment, click the menu icon and then click **Storage Classes** or **Blob Storage Tiering**.
2. Choose a storage class and then click **Save**.

Changing the free space ratio for data tiering

The free space ratio for data tiering defines how much free space is required on Cloud Volumes ONTAP SSDs/HDDs when tiering data to object storage. The default setting is 10% free space, but you can tweak the setting based on your requirements.

For example, you might choose less than 10% free space to ensure that you are utilizing the purchased capacity. Cloud Manager can then purchase additional disks for you when additional capacity is required (up until you reach the disk limit for the aggregate).

The ratio is important for disaster recovery scenarios because as data is read from the object store, Cloud Volumes ONTAP moves the data to SSDs/HDDs to provide better performance. If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data. Take this into consideration when changing the ratio so that you can meet your business requirements.



This setting applies to Cloud Volumes ONTAP only.

Steps

1. In the upper right of the Cloud Manager console, click the **Settings** icon, and select **Connector Settings**.



2. Under **Capacity**, click **Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering**.
3. Change the free space ratio based on your requirements and click **Save**.

Changing the cooling period for the auto tiering policy

If you enabled data tiering on a Cloud Volumes ONTAP volume using the *auto* tiering policy, you can adjust the default cooling period based on your business needs. This action is supported using the API only.

The cooling period is the number of days that user data in a volume must remain inactive before it is considered "cold" and moved to object storage.

The default cooling period for the auto tiering policy is 31 days. You can change the cooling period as follows:

- 9.8 or later: 2 days to 183 days
- 9.7 or earlier: 2 days to 63 days

Step

1. Use the *minimumCoolingDays* parameter with your API request when creating a volume or modifying an existing volume.

Using Cloud Volumes ONTAP as persistent storage for Kubernetes

Cloud Manager can automate the deployment of NetApp Trident on Kubernetes clusters so you can use Cloud Volumes ONTAP as persistent storage for containers.

Trident is a fully-supported open source project maintained by NetApp. Trident integrates natively with Kubernetes and its Persistent Volume framework to seamlessly provision and manage volumes from systems running any combination of NetApp's storage platforms. [Learn more about Trident](#).



The Kubernetes feature isn't supported with on-prem ONTAP clusters. It's supported with Cloud Volumes ONTAP only.

Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

1

Review prerequisites

Ensure that your environment can meet the prerequisites, which includes connectivity between Kubernetes clusters and Cloud Volumes ONTAP, connectivity between Kubernetes clusters and a Connector, a minimum Kubernetes version of 1.14, at least one worker node in a cluster, and more. [See the complete list](#).

2

Add your Kubernetes clusters to Cloud Manager

In Cloud Manager, click **K8s** and discover clusters directly from your cloud provider's managed service or import a cluster by providing a kubeconfig file.

3

Connect your clusters to Cloud Volumes ONTAP

After you add a Kubernetes cluster, click **Connect to Working Environment** to connect the cluster to one or more Cloud Volumes ONTAP systems.

4

Start provisioning Persistent Volumes

Request and manage Persistent Volumes using native Kubernetes interfaces and constructs. Cloud Manager creates NFS and iSCSI storage classes that you can use when provisioning Persistent Volumes.

[Learn more about provisioning your first volume with Trident for Kubernetes](#).

Reviewing prerequisites

Before you get started, ensure that your Kubernetes clusters and Connector meet specific requirements.

Kubernetes cluster requirements

- Network connectivity is required between a Kubernetes cluster and the Connector and between a Kubernetes cluster and Cloud Volumes ONTAP.

Both the Connector and Cloud Volumes ONTAP need a connection to the Kubernetes API endpoint:

- For managed clusters, set up a route between a cluster’s VPC and the VPC where the Connector and Cloud Volumes ONTAP reside.
- For other clusters, the IP address of the primary node or load balancer (as listed in the kubeconfig file) must be reachable by the Connector and Cloud Volumes ONTAP, and it must present a valid TLS certificate.
- A Kubernetes cluster can be in any location that has the network connectivity listed above.
- A Kubernetes cluster must be running version 1.14 at a minimum.

The maximum supported version is defined by Trident. [Click here to see the maximum supported Kubernetes version.](#)

- A Kubernetes cluster must have at least one worker node.
- For clusters running in Amazon Elastic Kubernetes Service (Amazon EKS), each cluster needs an IAM role added in order to resolve a permissions error. After you add the cluster, Cloud Manager will prompt you with the exact `eksctl` command that resolves the error.

[Learn about IAM permissions boundaries.](#)

- For clusters running in Azure Kubernetes Service (AKS), those clusters must be assigned the *Azure Kubernetes Service RBAC Cluster Admin* role. This is required so Cloud Manager can install Trident and configure storage classes on the cluster.
- For clusters running in Google Kubernetes Engine (GKE), those clusters must not use the default Container Optimized OS. You should switch them to use Ubuntu.

GKE defaults to using the Google [container-optimized image](#), which doesn’t have the utilities that Trident needs to mount volumes.

Connector requirements

Ensure that the following permissions are in place for the Connector.

Required permissions to discover and manage EKS clusters

The Connector needs Admin permissions to discover and manage Kubernetes clusters running in Amazon Elastic Kubernetes Service (EKS):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "eks:*",
            "Resource": "*"
        }
    ]
}
```

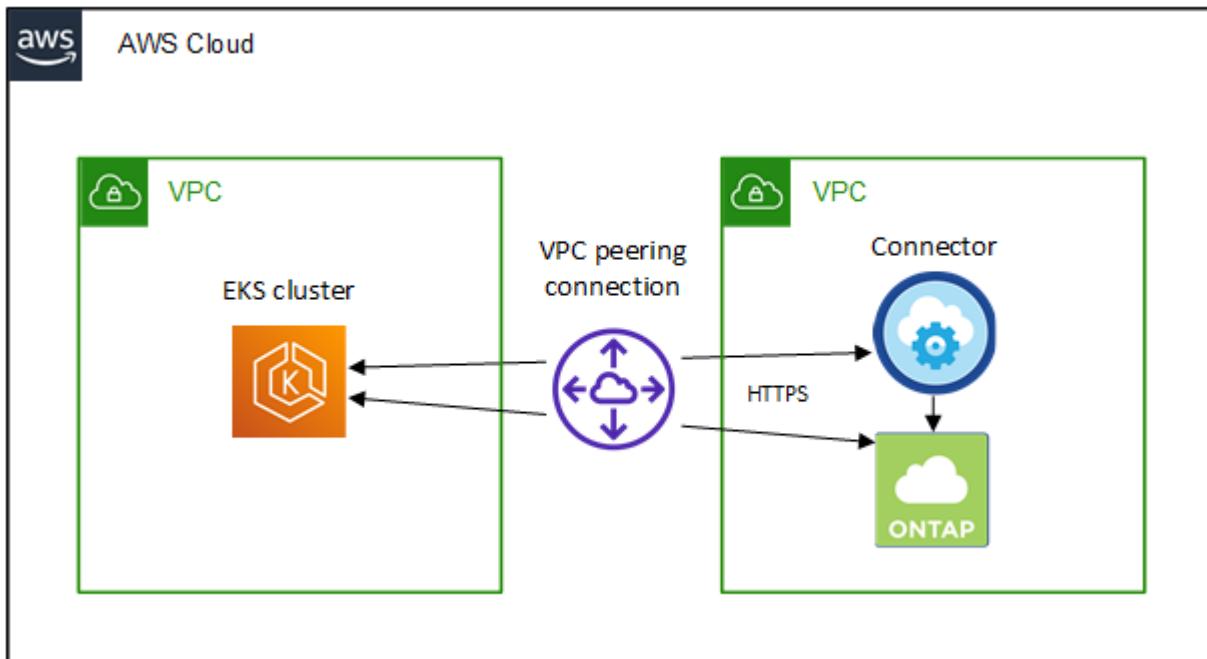
Required permissions to discover and manage GKE clusters

The Connector needs the following permissions to discover and manage Kubernetes clusters running in Google Kubernetes Engine (GKE):

```
container.*
```

Example setup

The following image shows an example of a Kubernetes cluster running in Amazon Elastic Kubernetes Service (Amazon EKS) and its connections to the Connector and Cloud Volumes ONTAP. In this example, VPC peering provides a connection between the VPC for the EKS cluster and the VPC for the Connector and Cloud Volumes ONTAP.



Adding Kubernetes clusters

Add Kubernetes clusters to Cloud Manager by discovering the clusters running in your cloud provider's managed Kubernetes service or by importing a cluster's kubeconfig file.

Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click **Add Cluster**.
3. Choose one of the available options:
 - Click **Discover Clusters** to discover the managed clusters that Cloud Manager has access to based on permissions that you provided to the Connector.

For example, if your Connector is running in Google Cloud, Cloud Manager uses the permissions from the Connector's service account to discover clusters running in Google Kubernetes Engine (GKE).

- Click **Import Cluster** to import a cluster using a kubeconfig file.

After you upload the file, Cloud Manager verifies connectivity to the cluster and saves an encrypted copy of the kubeconfig file.

Result

Cloud Manager adds the Kubernetes cluster. You can now connect the cluster to Cloud Volumes ONTAP.

Connecting a cluster to Cloud Volumes ONTAP

Connect a Kubernetes cluster to Cloud Volumes ONTAP so you can use Cloud Volumes ONTAP as persistent storage for containers.

Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click **Connect to Working Environment** for the cluster that you just added.

Status	Cluster Name	Added By	Version	Working Environments	Date Added
✓	kubernetes	Import	v1.18.0	Connect to Working Environment	August 30, 2020

3. Select a working environment and click **Continue**.
4. Choose the NetApp storage class to use as the default storage class for the Kubernetes cluster and click **Continue**.

When a user creates a persistent volume, the Kubernetes cluster can use this storage class as the backend storage by default.

5. Choose whether to use default auto export policies or whether to add a custom CIDR block.

Select Storage Class Type

Working Environment Information

Name	ishai0ntap4k8
Connected Clusters	None
Region	asia-east1
Zones	asia-east1-a
High Availability	Not Supported
Storage Classes	NFS Single Node Default iSCSI Single Node

Export Policy Information

If you plan to use NFS volumes you will need to set an export policy to allow connectivity between your clusters and your volumes.

Use the default auto-export policies. (Suitable for most cases.)

OR

General Network CIDR ⓘ
0.0.0.0/0

6. Click **Add Working Environment**.

Result

Cloud Manager connects the working environment to the cluster, which can take up to 15 minutes.

Managing your clusters

Cloud Manager enables you to manage your Kubernetes clusters by changing the default storage class, upgrading Trident, and more.

Changing the default storage class

Make sure that you've set a Cloud Volumes ONTAP storage class as the default storage class so clusters use Cloud Volumes ONTAP as the backend storage.

Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click the name of the Kubernetes cluster.
3. In the **Storage Classes** table, click the actions menu on the far right for the storage class that you'd like to set as the default.

6 Storage Classes

Storage Class ID	Provisioner	Volumes	Labels	
Gp2	aws	0		...
NFS Single Node	NetApp	0		...
NFS High Availability Default	NetApp	0		...
iSCSI High Availability	NetApp	0		
iSCSI Single Node	NetApp	0		

Set as Default

4. Click **Set as Default**.

Upgrading Trident

You can upgrade Trident from Cloud Manager when a new version is available.

Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click the name of the Kubernetes cluster.
3. If a new version is available, click **Upgrade** next to the Trident version.

The screenshot shows the 'Cluster Details' page for a cluster named 'kubernetes-baldwin'. The page includes a header with 'Cluster List > Cluster Details >' and two buttons: 'Connect to Working Environment' and 'Remove Cluster'. Below the header, there's a summary table with columns: Status (Running), Cluster Version (1.15), Added by (Discovery), Volumes (2), VPC (vpc-0485a0b201c3a1f2d), Date Added (September 3, 2020), and Trident Version (v20.04). A red arrow points to the 'Upgrade' button in the Trident Version row. At the bottom right, it says 'Provider AWS'.

Updating the kubeconfig file

If you added your cluster to Cloud Manager by importing the kubeconfig file, you can upload the latest kubeconfig file to Cloud Manager at any time. You might do this if you've updated the credentials, if you've changed users or roles, or if something changed that affects the cluster, user, namespaces, or authentication.

Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click the name of the Kubernetes cluster.
3. Click **Update Kubeconfig**.
4. When prompted through your web browser, select the updated kubeconfig file and click **Open**.

Result

Cloud Manager updates information about the Kubernetes cluster based on the latest kubeconfig file.

Disconnecting a cluster

When you disconnect a cluster from Cloud Volumes ONTAP, you can no longer use that Cloud Volumes ONTAP system as persistent storage for containers. Existing Persistent Volumes are not deleted.

Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click the name of the Kubernetes cluster.
3. In the **Working Environments** table, click the actions menu on the far right for the working environment that you want to disconnect.

4. Click **Disconnect**.

Result

Cloud Manager disconnects the cluster from the Cloud Volumes ONTAP system.

Removing a cluster

Remove decommissioned clusters from Cloud Manager after you disconnect all working environments from the cluster.

Steps

1. At the top of Cloud Manager, click **K8s**.
2. Click the name of the Kubernetes cluster.
3. Click **Remove Cluster**.

Encrypting volumes with NetApp encryption solutions

Cloud Volumes ONTAP supports both NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE) with an external key manager. NVE and NAE are software-based solutions that enable (FIPS) 140-2-compliant data-at-rest encryption of volumes. [Learn more about these encryption solutions](#).

Starting with Cloud Volumes ONTAP 9.7, new aggregates will have NAE enabled by default after you set up an

external key manager. New volumes that aren't part of an NAE aggregate will have NVE enabled by default (for example, if you have existing aggregates that were created before setting up an external key manager).

Cloud Volumes ONTAP doesn't support onboard key management.

What you'll need

Your Cloud Volumes ONTAP system should be registered with NetApp support. Starting with Cloud Manager 3.7.1, a NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support.

- [Adding NetApp Support Site accounts to Cloud Manager](#)
- [Registering pay-as-you-go systems](#)



Cloud Manager doesn't install the NVE license on systems that reside in the China region.

Steps

1. Review the list of supported key managers in the [NetApp Interoperability Matrix Tool](#).



Search for the **Key Managers** solution.

2. [Connect to the Cloud Volumes ONTAP CLI](#).

3. Install SSL certificates and connect to the external key management servers.

[ONTAP 9 NetApp Encryption Power Guide: Configuring external key management](#)

Manage storage VMs

Manage storage VMs in Cloud Manager

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but some configurations support additional storage VMs.

Supported number of storage VMs

Multiple storage VMs are supported with Cloud Volumes ONTAP in AWS and in Azure with certain configurations. Go to the [Cloud Volumes ONTAP Release Notes](#) to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

Work with multiple storage VMs

Cloud Manager supports any additional storage VMs that you create from System Manager or the CLI.

For example, the following image shows how you can choose a storage VM when you create a volume.

Details & Protection

Storage VM Name

i

Volume Name

i

Size (GiB)

i

Snapshot Policy

v

i Default Policy

And the following image shows how you can choose a storage VM when replicating a volume to another system.

Destination Volume Name

Destination Storage VM Name

v

Destination Aggregate

v

Modify the name of the default storage VM

Cloud Manager automatically names the single storage VM that it creates for Cloud Volumes ONTAP. You can modify the name of the storage VM if you have strict naming standards. For example, you might want the name to match how you name the storage VMs for your ONTAP clusters.

If you created any additional storage VMs for Cloud Volumes ONTAP, then you can't rename the storage VMs from Cloud Manager. You'll need to do so directly from Cloud Volumes ONTAP by using System Manager or

the CLI.

Steps

1. From the working environment, click the menu icon, and then click **Information**.
2. Click the edit icon to the right of the storage VM name.

The screenshot shows the 'Working Environment Information' page for an ONTAP system. It displays the following details:

ONTAP	
Serial Number:	[REDACTED]
System ID:	system-id-capacitytest
Cluster Name:	capacitytest
ONTAP Version:	9.7RC1
Date Created:	Jul 6, 2020 07:42:02 am
Storage VM Name:	svm_capacitytest 

3. In the Modify SVM Name dialog box, change the name, and then click **Save**.

Manage storage VMs for disaster recovery

Cloud Manager doesn't provide any setup or orchestration support for storage VM disaster recovery. You must use System Manager or the CLI.

- [SVM Disaster Recovery Preparation Express Guide](#)
- [SVM Disaster Recovery Express Guide](#)

Create data-serving storage VMs for Cloud Volumes ONTAP in AWS

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but some configurations support additional storage VMs.

To create additional data-serving storage VMs, you need to allocate IP addresses in AWS and then run ONTAP commands based on your Cloud Volumes ONTAP configuration.

Supported number of storage VMs

Multiple storage VMs are supported with Cloud Volumes ONTAP BYOL in AWS with an add-on license, starting with the 9.7 release. Go to the [Cloud Volumes ONTAP Release Notes](#) to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All other Cloud Volumes ONTAP configurations support one data-serving storage VM and one destination storage VM used for disaster recovery. You can activate the destination storage VM for data access if there's an outage on the source storage VM.

Verify limits for your configuration

Each EC2 instance supports a maximum number of private IPv4 addresses per network interface. You need to verify the limit before you allocate IP addresses in AWS for the new storage VM.

Steps

1. Go the [Storage limits section in the Cloud Volumes ONTAP Release Notes](#).
2. Identify the maximum number of IP addresses per interface for your instance type.
3. Make note of this number because you'll need it in the next section when you allocate IP addresses in AWS.

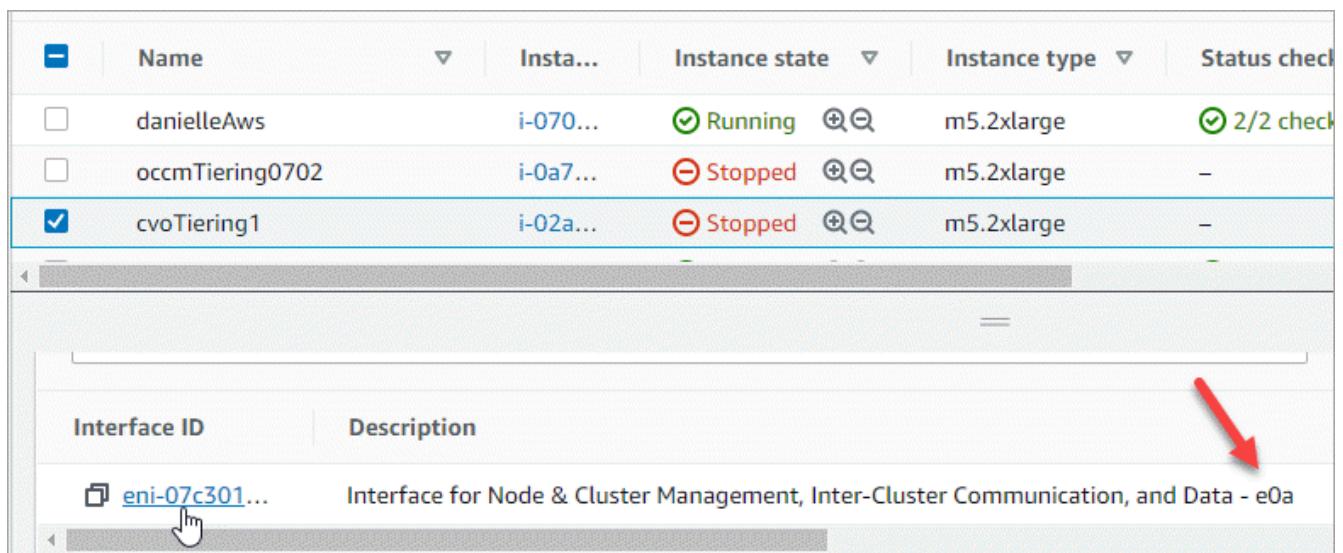
Allocate IP addresses in AWS

Private IPv4 addresses must be assigned to port e0a in AWS before you create LIFs for the new storage VM.

Note that an optional management LIF for a storage VM requires a private IP address on a single node system and on an HA pair in a single AZ. This management LIF provides a connection to management tools like SnapCenter.

Steps

1. Log in to AWS and open the EC2 service.
2. Select the Cloud Volumes ONTAP instance and click **Networking**.
If you're creating a storage VM on an HA pair, select node 1.
3. Scroll down to **Network interfaces** and click the **Interface ID** for port e0a.



4. Select the network interface and click **Actions > Manage IP addresses**.
5. Expand the list of IP addresses for e0a.
6. Verify the IP addresses:
 - a. Count the number of allocated IP addresses to confirm that the port has room for additional IPs.

You should have identified the maximum number of supported IP addresses per interface in the previous section of this page.
 - b. Optional: Go to the CLI for Cloud Volumes ONTAP and run **network interface show** to confirm that each of these IP addresses are in use.

If an IP address isn't in use, then you can use it with the new storage VM.
7. Back in the AWS Console, click **Assign new IP address** to assign additional IP addresses based on the amount that you need for the new storage VM.
 - Single node system: One unused secondary private IP is required.

An optional secondary private IP is required if you want to create a management LIF on the storage VM.
 - HA pair in a single AZ: One unused secondary private IP is required on node 1.

An optional secondary private IP is required if you want to create a management LIF on the storage VM.
 - HA pair in multiple AZs: One unused secondary private IP is required on each node.
8. If you're allocating the IP address on an HA pair in a single AZ, enable **Allow secondary private IPv4 addresses to be reassigned**.
9. Click **Save**.
10. If you have an HA pair in multiple AZs, then you'll need to repeat these steps for node 2.

Create a storage VM on a single node system

These steps create a new storage VM on a single node system. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. Create a NAS LIF.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node
```

Where *private_ip_x* is an unused secondary private IP on e0a.

3. Optional: Create a storage VM management LIF.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

Where *private_ip_y* is another unused secondary private IP on e0a.

Create a storage VM on an HA pair in a single AZ

These steps create a new storage VM on an HA pair in a single AZ. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

Both of these LIFs get allocated on node 1. The private IP addresses can move between nodes if failures occur.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

Where *private_ip_x* is an unused secondary private IP on e0a of cvo-node1. This IP address can be relocated to the e0a of cvo-node2 in case of takeover because the service policy default-data-files indicates that IPs can migrate to the partner node.

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

Where *private_ip_y* is another unused secondary private IP on e0a.

Create a storage VM on an HA pair in multiple AZs

These steps create a new storage VM on an HA pair in multiple AZs.

A *floating* IP address is required for a NAS LIF and is optional for a management LIF. These floating IP addresses don't require you to allocate private IPs in AWS. Instead, the floating IPs are automatically configured in the AWS route table to point to a specific node's ENI in the same VPC.

In order for floating IPs to work with ONTAP, a private IP address must be configured on every storage VM on each node. This is reflected in the steps below where an iSCSI LIF is created on node 1 and on node 2.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

- The floating IP address must be outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. 192.168.209.27 is an example floating IP address. [Learn more about choosing a floating IP address](#).
- `-service-policy default-data-files` indicates that IPs can migrate to the partner node.

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. Create an iSCSI LIF on node 1.

```
network interface create -vserver svm_2 -service-policy default-data-blocks -home-port e0a -address private_ip -netmask node1Mask -lif ip_node1_iscsi_2 -home-node cvo-node1
```

- This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
- `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.
- `private_ip` is an unused secondary private IP address on eth0 (e0a) of cvo_node1.

5. Create an iSCSI LIF on node 2.

```
network interface create -vserver svm_2 -service-policy default-data-blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif ip_node2_iscsi_2 -home-node cvo-node2
```

- This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
- `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.
- `private_ip` is an unused secondary private IP address on eth0 (e0a) of cvo_node2.

Create data-serving storage VMs for Cloud Volumes ONTAP in Azure

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but additional storage VMs are supported when running Cloud Volumes ONTAP in Azure.

To create additional data-serving storage VMs, you need to allocate IP addresses in Azure and then run ONTAP commands to create the storage VM and data LIFs.

Supported number of storage VMs

Multiple storage VMs are supported with Cloud Volumes ONTAP BYOL in Azure with an add-on license starting with the 9.9.0 release. Go to the [Cloud Volumes ONTAP Release Notes](#) to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All other Cloud Volumes ONTAP configurations support one data-serving storage VM and one destination storage VM used for disaster recovery. You can activate the destination storage VM for data access if there's an outage on the source storage VM.

Allocate IP addresses in Azure

Follow the steps below for your configuration: either a single node system, an HA pair using iSCSI, or an HA pair using NFS/SMB.

Single node

IP addresses must be assigned to nic0 in Azure before you create a storage VM and allocate LIFs.

You'll need to create an IP address for data LIF access and another optional IP address for a storage VM (SVM) management LIF. This management LIF provides a connection to management tools like SnapCenter.

Steps

1. Log in to the Azure portal and open the **Virtual machine** service.
2. Click the name of the Cloud Volumes ONTAP VM.
3. Click **Networking**.
4. Click the name of the network interface for nic0.
5. Under **Settings**, click **IP configurations**.
6. Click **Add**.
7. Enter a name for the IP configuration, select **Dynamic**, and then click **OK**.
8. Click the name of the IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.
9. If you want to create an SVM management LIF, repeat these steps on node 1.

After you finish

Copy the private IP addresses that you just created. You'll need to specify those IP addresses when you create LIFs for the new storage VM.

HA pair using iSCSI

iSCSI IP addresses must be assigned to nic0 in Azure before you create a storage VM and allocate LIFs. IPs for iSCSI are assigned to nic0 and not the load balancer because iSCSI uses ALUA for failover.

You'll need to create an IP address for data LIF access from node 1, another IP address for data LIF access from node 2, and another optional IP address for a storage VM (SVM) management LIF. This management LIF provides a connection to management tools like SnapCenter.

Steps

1. Log in to the Azure portal and open the **Virtual machine** service.
2. Click the name of the Cloud Volumes ONTAP VM for node 1.
3. Click **Networking**.
4. Click the name of the network interface for nic0.
5. Under **Settings**, click **IP configurations**.
6. Click **Add**.
7. Enter a name for the IP configuration, select **Dynamic**, and then click **OK**.
8. Click the name of the IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.
9. Repeat these steps on node 2.
10. If you want to create an SVM management LIF, repeat these steps on node 1.

After you finish

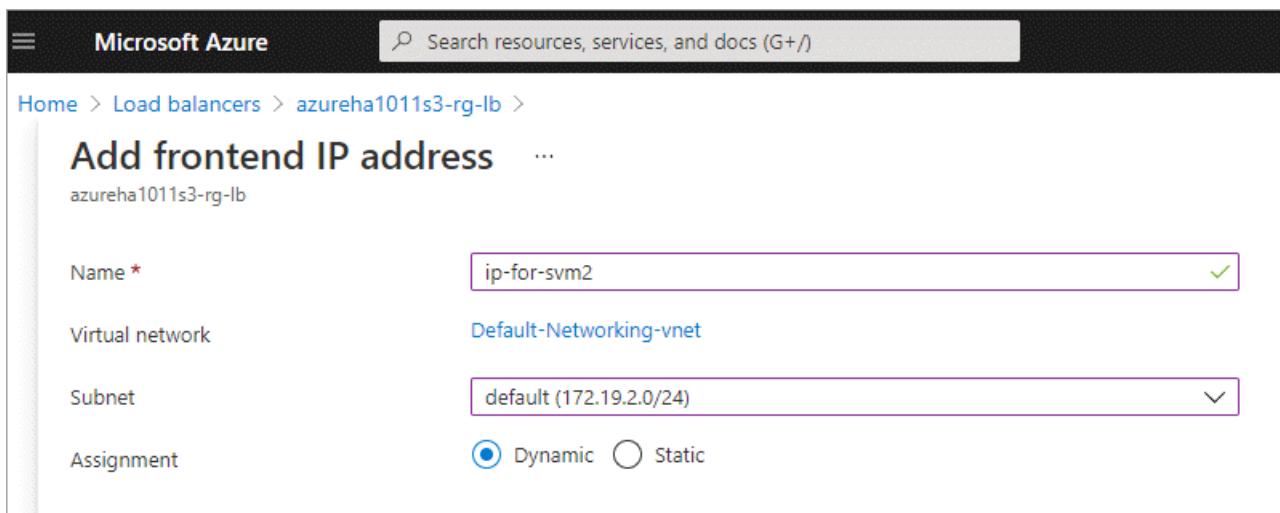
Copy the private IP addresses that you just created. You'll need to specify those IP addresses when you create LIFs for the new storage VM.

HA pair using NFS/SMB

IP addresses that you use for NFS and SMB data are allocated in the load balancer so that the IP addresses can migrate to the other node in case failover events occur.

Steps

1. In the Azure portal, open the **Load balancers** service.
2. Click the name of the load balancer for the HA pair.
3. Create one frontend IP configuration for data LIF access from node 1, another for data LIF access from node 2 (HA pairs only), and another optional frontend IP for a storage VM (SVM) management LIF.
 - a. Under **Settings**, click **Frontend IP configuration**.
 - b. Click **Add**.
 - c. Enter a name for the frontend IP, select the subnet for the Cloud Volumes ONTAP HA pair, and leave **Dynamic** selected.



- d. Click the name of the frontend IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.
4. Add a health probe for each frontend IP that you just created.
 - a. Under the load balancer's **Settings**, click **Health probes**.
 - b. Click **Add**.
 - c. Enter a name for the health probe and enter a port number that's between 63005 and 65000. Keep the default values for the other fields.

It's important that the port number is between 63005 and 65000. For example, if you are creating three health probes, you could enter probes that use the port numbers 63005, 63006, and 63007.

Microsoft Azure

Search resources, services, and

Home > Load balancers > azureha1011s3-rg-lb >

Add health probe

azureha1011s3-rg-lb

Name *	svm2-health-probe1	✓
Protocol *	TCP	▼
Port *	63005	✓
Interval *	5	seconds
Unhealthy threshold *	2	consecutive failures
Used by	Not used	

5. Create new load balancing rules for each frontend IP.

- Under the load balancer's **Settings**, click **Load balancing rules**.
- Click **Add** and enter the required information:
 - Name:** Enter a name for the rule.
 - IP Version:** Select **IPv4**.
 - Frontend IP address:** Select one of the frontend IP addresses that you just created.
 - HA Ports:** Enable this option.
 - Backend pool:** Keep the default Backend pool that was already selected.
 - Health probe:** Select the health probe that you created for the selected frontend IP.
 - Session persistence:** Select **None**.
 - Floating IP:** Select **Enabled**.

Add load balancing rule

chandanaTcpRst3-rg-lb

ⓘ A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *

jimmy_new_rule



IP Version *

IPv4 IPv6

Frontend IP address *

10.1.0.156 (dataAFIP)



HA Ports

Backend pool

backendPool (2 virtual machines)



Health probe

dataAProbe (TCP:63002)



Session persistence

None



Floating IP

Disabled Enabled

After you finish

Ensure that the network security group rules for Cloud Volumes ONTAP allows the load balancer to send TCP probes for the health probes that were created in step 4 above. Note that this is allowed by default.

Create a storage VM and LIFs

These steps create a new storage VM on a single node system or on an HA pair. One IP address is required for data LIF access from node 1, another IP address for data LIF access from node 2 (HA pairs only), and another optional IP address for a storage VM (SVM) management LIF. This management LIF provides a connection to management tools like SnapCenter.

Use the commands below that match the data access protocol for the storage VM, which is either NAS or iSCSI.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```

2. Create data LIFs:

- Use the following command to create a NAS LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask <length> -home-node <name-of-node1> -status-admin up -failover-policy system-defined -firewall-policy data -home-port e0a -auto-revert true -failover-group Default -probe-port <port-number-for-azure-health-probe1>
```

If this is a single node system, then you should change the value of the -failover-policy parameter to *disabled*.

- Use the following command to create a NAS LIF on node 2 (for HA pairs only).

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address> -netmask <length> -home-node <name-of-node2> -status-admin up -failover-policy system-defined -firewall-policy data -home-port e0a -auto-revert true -failover-group Default -probe-port <port-number-for-azure-health-probe2>
```

- Use the following command to create an iSCSI LIF on node 1.

```
network interface create -vserver <svm-name> -home-port e0a -address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

- Use the following command to create an iSCSI LIF on node 2 (for HA pairs only).

```
network interface create -vserver <svm-name> -home-port e0a -address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data  
-data-protocol none -address <svm-mgmt-ip-address> -netmask-length  
<length> -home-node node1 -status-admin up -failover-policy system-  
defined -firewall-policy mgmt -home-port e0a -auto-revert false  
-failover-group Default -probe-port <port-number-for-azure-health-  
probe3>
```

Monitor performance

Learn about the Monitoring service

The Monitoring service gives you insights into the health and performance of your Cloud Volumes ONTAP instances and helps you troubleshoot and optimize the performance of your cloud storage environment.

Features

- Automatically monitor all volumes
- View volume performance data in terms of IOPS, throughput, and latency
- Identify performance issues to minimize impact on your users and apps

Supported cloud providers

The Monitoring service is supported with Cloud Volumes ONTAP for AWS and Cloud Volumes ONTAP for Azure.

Cost

NetApp doesn't charge you for using the Monitoring service, but Cloud Manager launches a virtual machine in your VPC to facilitate monitoring. This VM results in charges from your cloud provider.

How the Monitoring service works

Cloud Manager leverages [NetApp's Cloud Insights service](#) to provide monitoring.

At a high-level, Cloud Insights integration with Cloud Manager works like this:

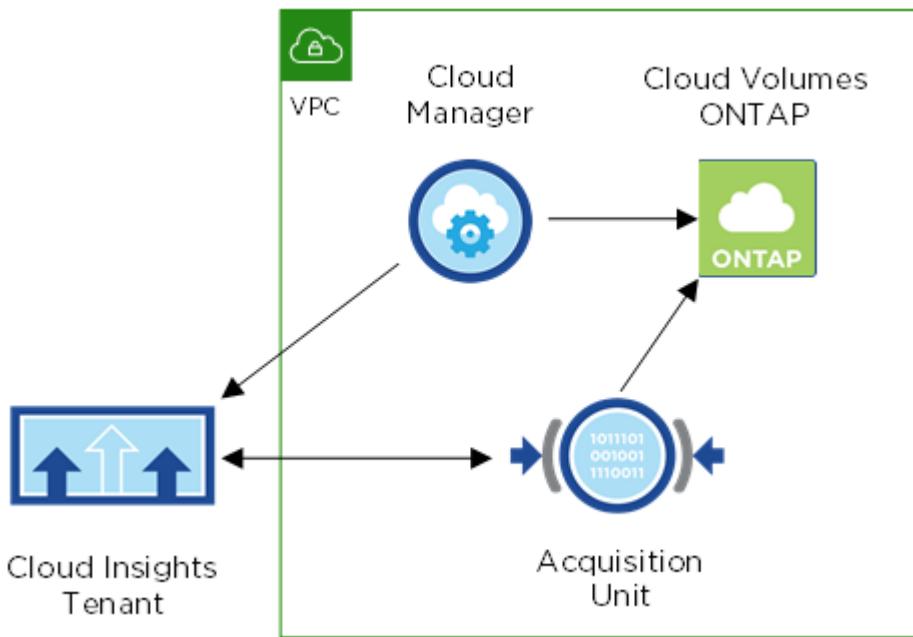
1. You enable the Monitoring service on Cloud Volumes ONTAP.
2. Cloud Manager configures your environment. It does the following:
 - a. Creates a Cloud Insights tenant (also called *environment*) and associates all users in your Cloud Central account to the tenant.

If you already have a tenant, then Cloud Manager uses that existing tenant.
 - b. Enables a free trial of Cloud Insights.

On the 29th day, your plan automatically transitions from the Trial Version to the [Basic Edition](#).

- c. Deploys a virtual machine in your VPC/VNet called an Acquisition Unit. The Acquisition Unit facilitates monitoring of volumes (this is the VM mentioned in the Cost section above).
 - d. Connects the Acquisition Unit to Cloud Volumes ONTAP and to the Cloud Insights tenant.
3. In Cloud Manager, you click Monitoring and use the performance data to troubleshoot and optimize performance.

The following image shows the relationship between these components in an AWS VPC:



The Acquisition Unit

When you enable Monitoring, Cloud Manager deploys an Acquisition Unit in the same subnet as the Connector.

An *Acquisition Unit* collects performance data from Cloud Volumes ONTAP and sends it to the Cloud Insights tenant. Cloud Manager then queries that data and presents it to you.

Note the following about the Acquisition Unit instance:

- In AWS, the Acquisition Unit runs on a t3.xlarge instance with a 100 GB GP2 volume.
- In Azure, the Acquisition Unit runs on a D4_v3 virtual machine with a 30 GB Standard SSD.
- The instance is named *CloudInsights-AU* with a generated hash (UUID) concatenated to it. For example: *CloudInsights-AU-FAN7FqeH*
- Only one Acquisition Unit is deployed per Connector.
- The instance must be running to access performance information in the Monitoring tab.

Cloud Insights tenant

If you don't already have a *tenant*, Cloud Manager sets one up for you when you enable Monitoring. A Cloud Insights tenant enables you to access the performance data that the Acquisition Unit collects. The tenant is a secure data partition within the NetApp Cloud Insights service.

Cloud Insights web interface

The Monitoring tab in Cloud Manager provides basic performance data for your volumes. You can go to the Cloud Insights web interface from your browser to perform more in-depth monitoring and to configure alerts for your Cloud Volumes ONTAP systems.

Free trial and subscription

Cloud Manager enables a free trial of Cloud Insights to provide performance data within Cloud Manager and for you to explore the features that Cloud Insights Standard Edition has to offer.

On the 29th day, your plan automatically transitions from the Trial Version to the [Basic Edition](#).

You have the option to subscribe to the Standard or Premium editions to gain access to additional features from the Cloud Insights web interface.

[Learn how to subscribe to Cloud Insights.](#)

Monitoring Cloud Volumes ONTAP

Complete a few steps to start monitoring Cloud Volumes ONTAP performance.

Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.



Verify support for your configuration

- You need a Cloud Volumes ONTAP system running in AWS or Azure.
- For AWS, you need a Connector running version 3.8.4 or later.
- For Azure, you need a Connector running version 3.9.3 or later.



Enable Monitoring on your new or existing system

- New working environments: Be sure to keep Monitoring enabled when you create the working environment (it's enabled by default).
- Existing working environments: Select a working environment and click **Start Monitoring**.



View performance data

Click **Monitoring** and view performance data for your volumes.

Requirements

Read the following requirements to make sure that you have a supported configuration.

Supported Cloud Volumes ONTAP versions

Any version of Cloud Volumes ONTAP in AWS or in Azure.

Supported Connector

- For AWS, you need a Connector running version 3.8.4 or later.
- For Azure, you need a Connector running version 3.9.3 or later.



You can view a Connector's version by clicking the icon and then **Support > Connector**.

Email address for Cloud Central

The email address for your Cloud Central user account should be your business email address. Free email domains like gmail and hotmail aren't supported when creating a Cloud Insights tenant.

Networking for the Acquisition Unit

The Acquisition Unit uses 2-way/mutual authentication to connect to the Cloud Insights server. The client certificate must be passed to the Cloud Insights server to be authenticated. To accomplish this, the proxy must be set up to forward the http request to the Cloud Insights server without decrypting the data.

The Acquisition Unit uses the following two endpoints to communicate with Cloud Insights. If you have a firewall between the Acquisition Unit server and Cloud Insights, you need these endpoints when configuring firewall rules:

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

For example:

```
https://aulogin.c01.cloudinsights.netapp.com
https://cg0c586a-ee05-45rb-a5ac-
333b5ae7718d7.c01.cloudinsights.netapp.com
```

Contact us through the in-product chat if you need help identifying your Cloud Insights domain and tenant ID.

Networking for the Connector

Similar to the Acquisition Unit, the Connector must have outbound connectivity to the Cloud Insights tenant. But the endpoint that the Connector contacts is slightly different. It contacts the tenant host URL using the shortened tenant ID:

```
https://<your-short-tenant-ID>.<Cloud Insights Domain>
```

For example:

```
https://abcd12345.c01.cloudinsights.netapp.com
```

Again, you can contact us through the in-product chat if you need help identifying the tenant host URL.

Enabling monitoring on a new system

The Monitoring service is enabled by default in the working environment wizard. Be sure to keep the option enabled.

Steps

1. Click **Create Cloud Volumes ONTAP**.
2. Select Amazon Web Services or Microsoft Azure as the cloud provider and then choose a single node or HA system.
3. Fill out the Details & Credentials page.
4. On the Services page, leave the Monitoring service enabled and click **Continue**.

The screenshot shows a configuration interface for the NetApp Monitoring service. At the top, there's a header with a monitoring icon and the word "Monitoring". To the right is a blue toggle switch that is turned on. Below the header, there's a descriptive text block: "NetApp Monitoring is an infrastructure monitoring tool that gives you visibility into your complete infrastructure. With Monitoring, you can monitor, troubleshoot and optimize all your resources including your public clouds and your private data centers." Underneath this text, there are two sections: "ADVANTAGES" and "CLARIFICATIONS", each containing a bulleted list of points.

ADVANTAGES	CLARIFICATIONS
<ul style="list-style-type: none">➤ Automatically monitor all volumes - no configuration is required➤ Prevent performance issues from impacting your users and apps	<ul style="list-style-type: none">➤ Activation is free, but requires deploying a small-size cloud instance which will incur charges by your cloud provider➤ Monitoring can be disabled at any time

Enabling monitoring on an existing system

Enable monitoring at any time from the working environment.

Steps

1. At the top of Cloud Manager, click **Canvas**.
2. Select a working environment.
3. In the pane on the right, click **Start Monitoring**.

The screenshot shows the Cloud Manager interface with the following details:

- CVO2**: Status is **On | AWS**. Action buttons: **i**, **⋮**, **X**.
- SERVICES** section:
 - Cloud Compliance**: Status is **Off**. Action button: **Enable Compliance**.
 - Backup to Cloud**: Status is **On**. Information: **1 Volume Backed Up**. Action button: **⋮**.
 - Kubernetes**: Status is **Off**. Action button: **Activate Kubernetes**.
 - Monitoring**: Status is **Off**. Action button: **Start Monitoring** (with a hand cursor icon).

Monitoring your volumes

Monitor performance by viewing IOPS, throughput, and latency for each of your volumes.

Steps

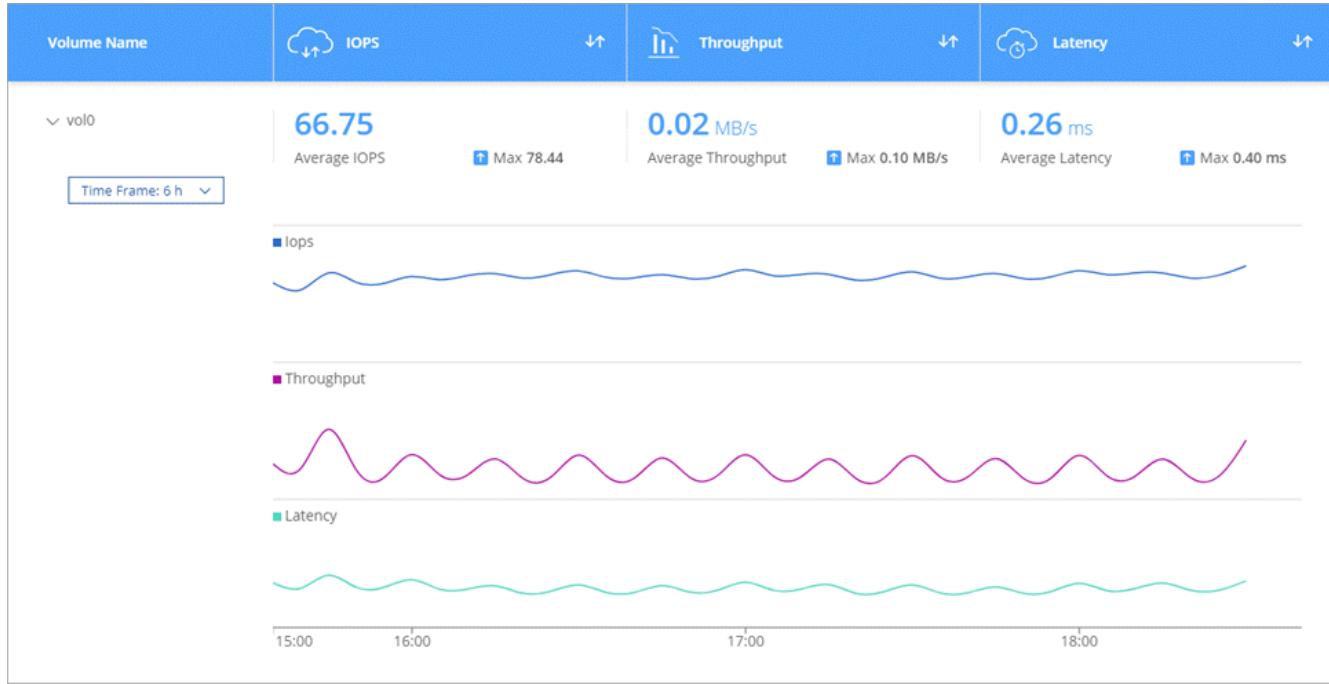
1. At the top of Cloud Manager, click **Monitoring**.
2. Filter the contents of the dashboard to get the information that you need.
 - Select a specific working environment.
 - Select a different timeframe.
 - Select a specific SVM.
 - Search for a specific volume.

The following image highlights each of these options:

The screenshot shows the Cloud Manager interface with the 'Monitoring' tab selected. At the top, there are two status cards: '0.02 MB/s Average Network Throughput' and '5.55 % Average CPU Utilization'. Below these are two volume cards: 'vol0' with IOPS 66.75, Throughput 0.02 MB/s, and Latency 0.26 ms; and 'volaws2' with IOPS 50.02, Throughput 12.60 MB/s, and Latency 0.19 ms. A search bar and a table header with columns for Volume Name, IOPS, Throughput, and Latency are also visible.

Volume Name	IOPS	Throughput	Latency
> vol0	66.75 Average IOPS	0.02 MB/s Average Throughput	0.26 ms Average Latency
> volaws2	50.02 Average IOPS	12.60 MB/s Average Throughput	0.19 ms Average Latency

- Click a volume in the table to expand the row and view a timeline for IOPS, throughput, and latency.



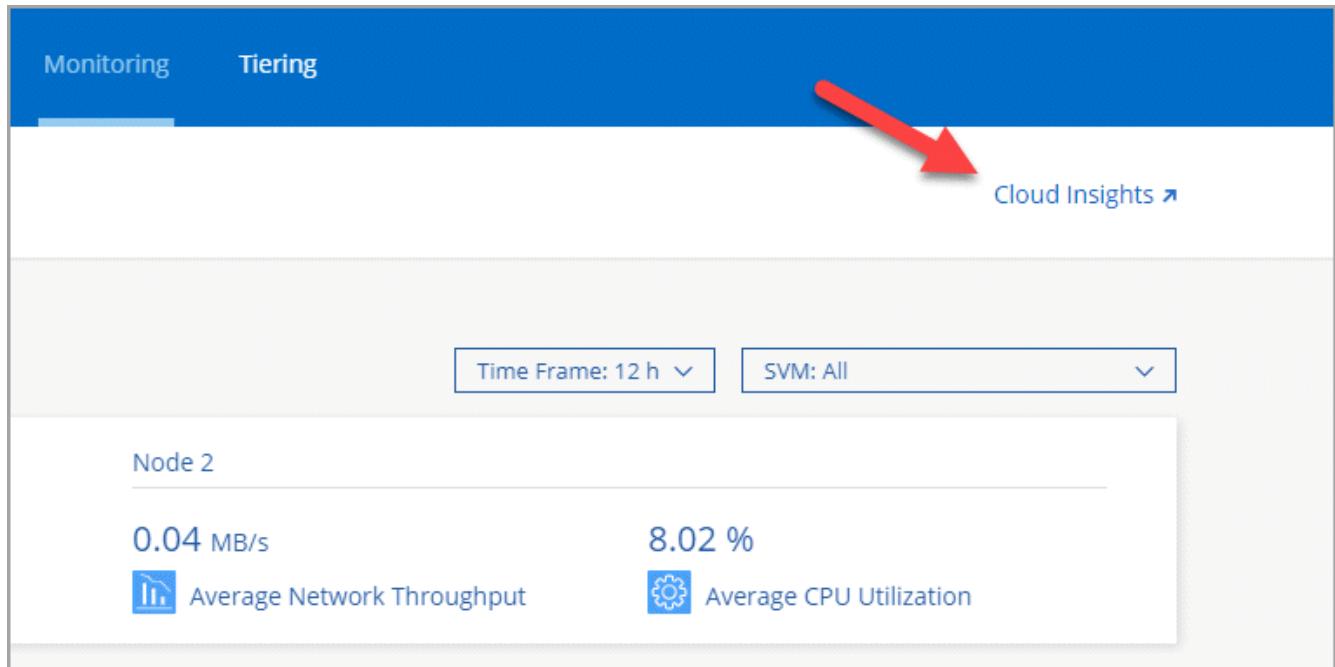
- Use the data to identify performance issues to minimize impact on your users and apps.

Getting more information from Cloud Insights

The Monitoring tab in Cloud Manager provides basic performance data for your volumes. You can go to the Cloud Insights web interface from your browser to perform more in-depth monitoring and to configure alerts for your Cloud Volumes ONTAP systems.

Steps

- At the top of Cloud Manager, click **Monitoring**.
- Click the **Cloud Insights** link.



Result

Cloud Insights open in a new browser tab. If you need help, refer to the [Cloud Insights documentation](#).

Disabling monitoring

If you no longer want to monitor Cloud Volumes ONTAP, you can disable the service at any time.



If you disable monitoring from each of your working environments, you'll need to delete the virtual machine instance yourself. The instance is named *AcquisitionUnit* with a generated hash (UUID) concatenated to it. For example: *AcquisitionUnit-FAN7FqeH*

Steps

1. At the top of Cloud Manager, click **Canvas**.
2. Select a working environment.
3. In the pane on the right, click the icon and select **Deactivate Scan**.

Improving protection against ransomware

Ransomware attacks can cost a business time, resources, and reputation. Cloud Manager enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

Steps

1. From the working environment, click the **Ransomware** icon.

2. Implement the NetApp solution for ransomware:

- Click **Activate Snapshot Policy**, if you have volumes that do not have a Snapshot policy enabled.

NetApp Snapshot technology provides the industry's best solution for ransomware remediation. The key to a successful recovery is restoring from uninfected backups. Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

- Click **Activate FPolicy** to enable ONTAP's FPolicy solution, which can block file operations based on a file's extension.

This preventative solution improves protection from ransomware attacks by blocking common ransomware file types.

The default FPolicy scope blocks files that have the following extensions:

micro, encrypted, locked, crypto, crypt, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, good, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre



Cloud Manager creates this scope when you activate FPolicy on Cloud Volumes ONTAP. The list is based on common ransomware file types. You can customize the blocked file extensions by using the `vserver fpolicy policy scope` commands from the Cloud Volumes ONTAP CLI.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection ⓘ



1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes ⓘ

[Activate Snapshot Policy](#)

2 Block Ransomware File Extensions ⓘ



ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names](#) ⓘ

[Activate FPolicy](#)

Administer

Manage licenses for Cloud Volumes ONTAP

The Digital Wallet page enables you to manage licenses for Cloud Volumes ONTAP from a single location. You can add new licenses and update existing licenses.

You can manage the following types of licenses for Cloud Volumes ONTAP:

- *Capacity-based licenses*, which enable you to pay for Cloud Volumes ONTAP per TiB of capacity.

[Contact NetApp Sales](#) to purchase a capacity-based license.

- *Node-based licenses*, which are any of the following:

- BYOL licenses purchased from NetApp.

This includes Eval licenses that you can later convert to BYOL licenses.

To get started with a node-based BYOL, [contact NetApp Sales](#).

- Hourly pay-as-you-go (PAYGO) subscriptions from your cloud provider's marketplace.

This includes 30-day free trials.

To get started with PAYGO, create a Cloud Volumes ONTAP working environment and subscribe to your cloud provider's marketplace when prompted.

[Learn more about Cloud Volumes ONTAP licenses.](#)

Manage capacity-based licenses

Manage your capacity-based licenses to ensure that your NetApp account has enough capacity for your Cloud Volumes ONTAP systems.

View your account's capacity

View the licensed capacity and provisioned capacity by package to ensure that you have enough room for your data volumes.

Steps

1. Click **All Services > Digital Wallet > Capacity-Based Licenses**.
2. View the licensed capacity and provisioned capacity for each package.

Serial Number	Package Type	Package Flavor	License Capacity	License Expiry	...
90120130000000000021	Professional	---	100 TB	January 1, 2022	...

3. If needed, purchase additional licensed capacity and then add the license to your account.

Add purchased licenses to your account

After you purchase licenses for your NetApp account, you need to add the licenses to Cloud Manager so that the capacity is available for Cloud Volumes ONTAP.

What you'll need

- You need to provide Cloud Manager the serial number of the license or the license file.
- If you want to enter the serial number, you first need to [add your NetApp Support Site account to Cloud Manager](#). This is the NetApp Support Site account that's authorized to access the serial number.

Steps

1. Click **All Services > Digital Wallet > Capacity-Based Licenses**.
2. Click **Add License**.
3. Enter the serial number for your capacity-based license or upload the license file.

If you entered a serial number, you also need to select the NetApp Support Site account that's authorized to access the serial number.

4. Click **Add License**.

Update a capacity-based license

If you purchased additional capacity or extended the term of your license, then you'll need to update the license in Cloud Manager.

What you'll need

The license file (or *files* if you have an HA pair).

Steps

1. Click **All Services > Digital Wallet > Capacity-Based Licenses**.
2. Click the action menu next to the license and select **Update License**.
3. Upload the license file.
4. Click **Upload License**.

Remove a capacity-based license

If a capacity-based license expired and is no longer in use, then you can remove it at any time.

Steps

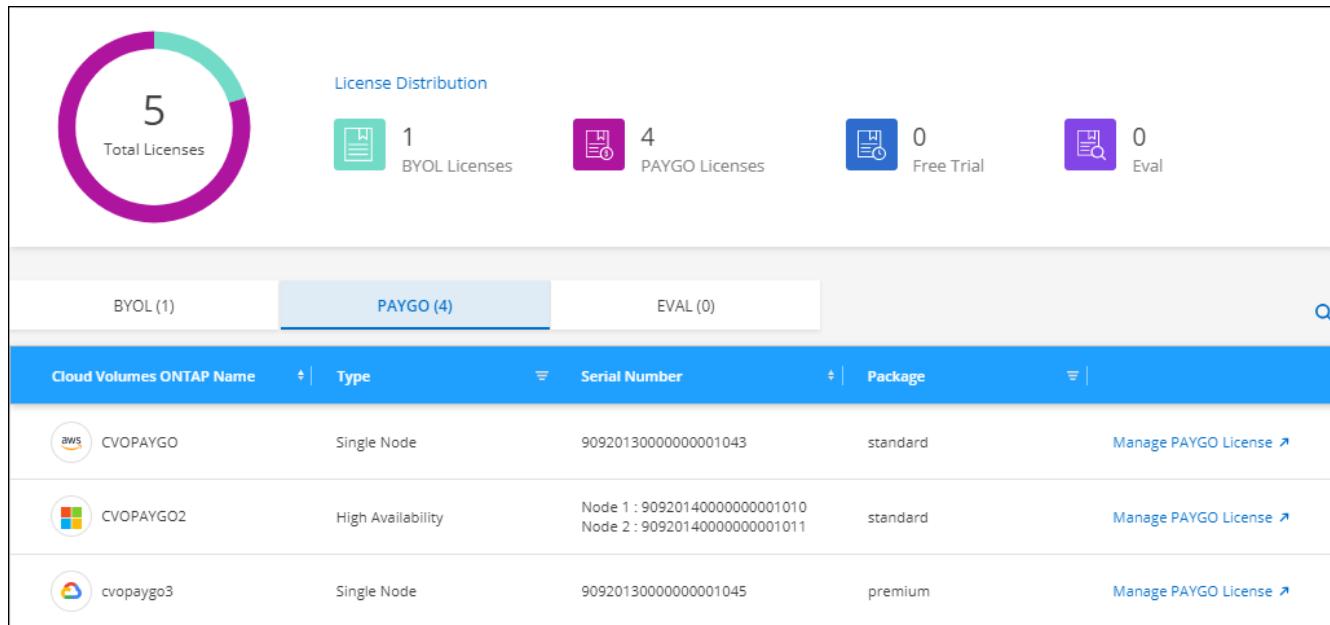
1. Click **All Services > Digital Wallet > Capacity-Based Licenses**.
2. Click the action menu next to the license and select **Remove License**.
3. Click **Remove** to confirm.

Manage node-based PAYGO licenses

The Digital Wallet page enables you to view details about each of your PAYGO Cloud Volumes ONTAP systems, including the serial number and PAYGO license type.

Steps

1. Click **All Services > Digital Wallet > Node-Based Licenses**.
2. Click **PAYGO**.
3. View details in the table about each of your PAYGO licenses.



4. If needed, click **Manage PAYGO License** to change the PAYGO license or to change the instance type.

Manage node-based BYOL licenses

Manage your node-based licenses to ensure that each Cloud Volumes ONTAP system has a valid license with the required capacity.

Obtain a system license file

In most cases, Cloud Manager can automatically obtain your license file using your NetApp Support Site account. But if it can't, then you'll need to manually upload the license file. If you don't have the license file, you can obtain it from netapp.com.

Steps

1. Go to the [NetApp License File Generator](#) and log in using your NetApp Support Site credentials.
2. Enter your password, choose your product, enter the serial number, confirm that you have read and accepted the privacy policy, and then click **Submit**.

Example

3. Choose whether you want to receive the serialnumber.NLF JSON file through email or direct download.

Update a system license

When you renew a BYOL subscription by contacting a NetApp representative, Cloud Manager automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system.

If Cloud Manager can't access the license file over the secure internet connection, you can obtain the file yourself and then manually upload the file to Cloud Manager.

Steps

1. Click **All Services > Digital Wallet > Node-Based Licenses**.
2. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
3. Click the action menu next to the system license and select **Update License**.
4. Upload the license file (or files if you have an HA pair).
5. Click **Update License**.

Result

Cloud Manager updates the license on the Cloud Volumes ONTAP system.

Manage extra capacity licenses

You can purchase extra capacity licenses for a Cloud Volumes ONTAP BYOL system to allocate more than the 368 TB of capacity that's provided with a BYOL system license. For example, you might purchase one extra license capacity to allocate up to 736 TB of capacity to Cloud Volumes ONTAP. Or you could purchase three extra capacity licenses to get up to 1.4 PB.

The number of licenses that you can purchase for a single node system or HA pair is unlimited.

Add capacity licenses

Purchase an extra capacity license by contacting us through the chat icon in the lower-right of Cloud Manager. After you purchase the license, you can apply it to a Cloud Volumes ONTAP system.

Steps

1. Click **All Services > Digital Wallet > Node-Based Licenses**.
2. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
3. Click **Add Capacity License**.
4. Enter the serial number or upload the license file (or files if you have an HA pair).
5. Click **Add Capacity License**.

Update capacity licenses

If you extended the term of an extra capacity license, you'll need to update the license in Cloud Manager.

Steps

1. Click **All Services > Digital Wallet > Node-Based Licenses**.
2. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
3. Click the action menu next to the capacity license and select **Update License**.
4. Upload the license file (or files if you have an HA pair).
5. Click **Update License**.

Remove capacity licenses

If an extra capacity license expired and is no longer in use, then you can remove it at any time.

Steps

1. Click **All Services > Digital Wallet > Node-Based Licenses**.
2. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
3. Click the action menu next to the capacity license and select **Remove License**.
4. Click **Remove**.

Convert an Eval license to BYOL

An evaluation license is good for 30 days. You can apply a new BYOL license on top of the evaluation license for an in-place upgrade (this requires a restart of single node systems).

[Learn more about Evaluation licenses.](#)

Steps

1. Click **All Services > Digital Wallet > Node-Based Licenses**.
2. Click **Eval**.
3. In the table, click **Convert to BYOL License** for a Cloud Volumes ONTAP system.
4. Enter the serial number or upload the license file.
5. Click **Convert License**.

Registering pay-as-you-go systems

Support from NetApp is included with Cloud Volumes ONTAP Explore, Standard, and Premium systems, but you must first activate support by registering the systems with NetApp.

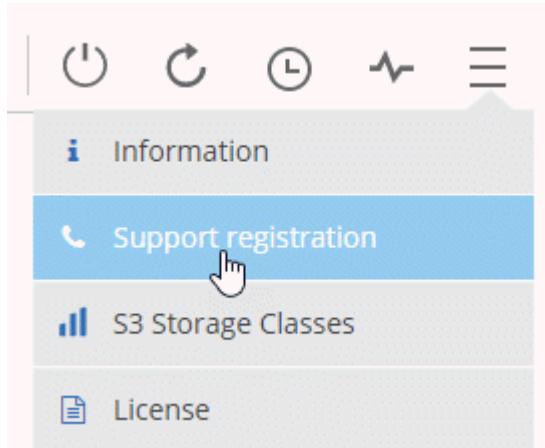
Registering a PAYGO system with NetApp is required to upgrade ONTAP software using any of the methods [described on this page](#).



A system that isn't registered for support will still receive the software update notifications that appear in Cloud Manager when a new version is available. But you will need to register the system before you can upgrade the software.

Steps

1. If you have not yet added your NetApp Support Site account to Cloud Manager, go to **Account Settings** and add it now.
[Learn how to add NetApp Support Site accounts.](#)
2. On the Canvas page, double-click the name of the system that you want to register.
3. Click the menu icon and then click **Support registration**:



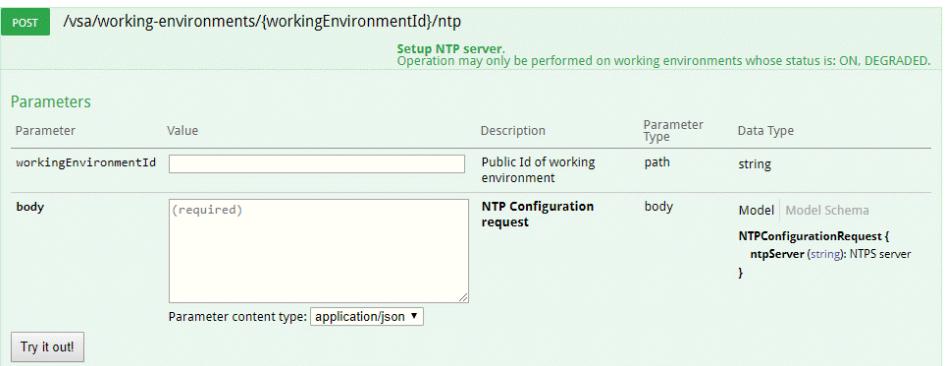
4. Select a NetApp Support Site account and click **Register**.

Result

Cloud Manager registers the system with NetApp.

Setting up Cloud Volumes ONTAP

After you deploy Cloud Volumes ONTAP, you can set it up by synchronizing the system time using NTP and by performing a few optional tasks from either System Manager or the CLI.

Task	Description
<p>Synchronize the system time using NTP</p>	<p>Specifying an NTP server synchronizes the time between the systems in your network, which can help prevent issues due to time differences.</p> <p>Specify an NTP server using the Cloud Manager API or from the user interface when you set up a CIFS server.</p> <ul style="list-style-type: none"> • Modifying the CIFS server • Cloud Manager automation docs <p>For example, here's the API for a single-node system in AWS:</p>  <pre> POST /vsa/working-environments/{workingEnvironmentId}/ntp Setup NTP server. Operation may only be performed on working environments whose status is: ON, DEGRADED. Parameters Parameter Value Description Parameter Type Data Type workingEnvironmentId [] Public Id of working environment path string body (required) NTP Configuration request body Model<NTPConfigurationRequest> NTPConfigurationRequest { ntpServer(string): NTPs server } Parameter content type: application/json ▾ Try it out! </pre>
<p>Optional: Configure AutoSupport</p>	<p>AutoSupport proactively monitors the health of your system and automatically sends messages to NetApp technical support by default.</p> <p>If the Account Admin added a proxy server to Cloud Manager before you launched your instance, Cloud Volumes ONTAP is configured to use that proxy server for AutoSupport messages.</p> <p>You should test AutoSupport to ensure that it can send messages. For instructions, see the System Manager Help or the ONTAP 9 System Administration Reference.</p>
<p>Optional: Configure the Cloud Manager Connector as the AutoSupport proxy</p>	<p>If your environment requires a proxy server to send AutoSupport messages, you can configure the Connector to act as the proxy. No configuration for the Connector is required, other than internet access. You simply need to go to the CLI for Cloud Volumes ONTAP and run the following command:</p> <pre>system node autosupport modify -proxy-url <connector-ip-address></pre>
<p>Optional: Configure EMS</p>	<p>The Event Management System (EMS) collects and displays information about events that occur on Cloud Volumes ONTAP systems. To receive event notifications, you can set event destinations (email addresses, SNMP trap hosts, or syslog servers) and event routes for a particular event severity.</p> <p>You can configure EMS using the CLI. For instructions, see the ONTAP 9 EMS Configuration Express Guide.</p>

Task	Description
Optional: Change the backup location of configuration files	<p>Cloud Volumes ONTAP automatically creates configuration backup files that contain information about the configurable options that it needs to operate properly.</p> <p>By default, Cloud Volumes ONTAP backs up the files to the Connector host every eight hours. If you want to send the backups to an alternate location, you can change the location to an FTP or HTTP server in your data center or in AWS. For example, you might already have a backup location for your FAS storage systems.</p> <p>You can change the backup location using the CLI. See the ONTAP 9 System Administration Reference.</p>

Upgrading Cloud Volumes ONTAP software

Cloud Manager includes several options that you can use to upgrade to the current Cloud Volumes ONTAP release. You should prepare Cloud Volumes ONTAP systems before you upgrade the software.

Requirements

You should be aware of the following requirements before you start the Cloud Volumes ONTAP upgrade process.

Software upgrades must be completed by Cloud Manager

Upgrades of Cloud Volumes ONTAP must be completed from Cloud Manager. You should not upgrade Cloud Volumes ONTAP by using System Manager or the CLI. Doing so can impact system stability.

Cloud Volumes ONTAP must be registered with NetApp Support

Cloud Volumes ONTAP must be registered with NetApp support in order to upgrade the software using any of the methods described on this page. This applies to both PAYGO and BYOL. You'll need to [manually register PAYGO systems](#), while BYOL systems are registered by default.



A system that isn't registered for support will still receive the software update notifications that appear in Cloud Manager when a new version is available. But you will need to register the system before you can upgrade the software.

A note about downgrades

Cloud Manager doesn't support downgrading Cloud Volumes ONTAP to a previous version. Contact NetApp technical support for help with downgrades.

Ways to upgrade Cloud Volumes ONTAP

Cloud Manager displays a notification in Cloud Volumes ONTAP working environments when a new version of Cloud Volumes ONTAP is available:

The screenshot shows the Cloud Manager dashboard. At the top, there's a cloud icon and the text "Visual View". Below it, a system card for "cloudvolumesontap1" is shown, indicating it is "On | AWS". The card has three icons: a blue circle with a white "i", a grey circle with three dots, and a grey circle with an "X". Underneath the card, a red box highlights the "NOTIFICATIONS" section. Inside this section, there's a message with a blue star icon followed by the text "New version available" and a small grey arrow icon to its right. Below the notifications, there's a "SERVICES" section with two items: "Cloud Compliance" (status "On") and "No Personal Files Found".

You can start the upgrade process from this notification, which automates the process by obtaining the software image from an S3 bucket, installing the image, and then restarting the system. For details, see [Upgrading Cloud Volumes ONTAP from Cloud Manager notifications](#).



For HA systems in AWS, Cloud Manager might upgrade the HA mediator as part of the upgrade process.

Cloud Manager also provides the following advanced options for upgrading Cloud Volumes ONTAP software with both PAYGO and BYOL:

- Software upgrades using an image on an external URL

This option is helpful if Cloud Manager can't access the S3 bucket to upgrade the software or if you were provided with a patch.

For details, see [Upgrading Cloud Volumes ONTAP by using an HTTP or FTP server](#).

- Software upgrades using the alternate image on the system

You can use this option to upgrade by making the alternate software image the default image. This option is not available for HA pairs.

For details, see [Upgrading Cloud Volumes ONTAP by using a local image](#).

Preparing to upgrade Cloud Volumes ONTAP software

Before performing an upgrade, you must verify that your systems are ready and make any required configuration changes.

- Understanding supported upgrade paths
- Planning for downtime
- Verifying that automatic giveback is still enabled
- Suspending SnapMirror transfers
- Verifying that aggregates are online

Understanding supported upgrade paths

Refer to the "Upgrade notes" page in the Cloud Volumes ONTAP Release Notes for the target version.

Planning for downtime

When you upgrade a single-node system, the upgrade process takes the system offline for up to 25 minutes, during which I/O is interrupted.

Upgrading an HA pair is nondisruptive and I/O is uninterrupted. During this nondisruptive upgrade process, each node is upgraded in tandem to continue serving I/O to clients.

Verifying that automatic giveback is still enabled

Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

[ONTAP 9 Documentation: Commands for configuring automatic giveback](#)

Suspending SnapMirror transfers

If a Cloud Volumes ONTAP system has active SnapMirror relationships, it is best to suspend transfers before you update the Cloud Volumes ONTAP software. Suspending the transfers prevents SnapMirror failures. You must suspend the transfers from the destination system.



Even though Cloud Backup uses an implementation of SnapMirror to create backup files (called SnapMirror Cloud), backups do not need to be suspended when a system is upgraded.

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. [Log in to System Manager](#) from the destination system.
2. Click **Protection > Relationships**.
3. Select the relationship and click **Operations > Quiesce**.

Verifying that aggregates are online

Aggregates for Cloud Volumes ONTAP must be online before you update the software. Aggregates should be online in most configurations, but if they are not, then you should bring them online.

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
2. Select an aggregate, click **Info**, and then verify that the state is online.

The screenshot shows a summary of aggregate 'aggr1'. It includes the following details:

- Aggregate Capacity: 88.57 GB
- Used Aggregate Capacity: 1.07 GB
- Volumes: 2
- AWS Disks: 1
- State: online

3. If the aggregate is offline, use System Manager to bring the aggregate online:
 - a. [Log in to System Manager](#).
 - b. Click **Storage > Aggregates & Disks > Aggregates**.
 - c. Select the aggregate, and then click **More Actions > Status > Online**.

Upgrading Cloud Volumes ONTAP from Cloud Manager notifications

Cloud Manager notifies you when a new version of Cloud Volumes ONTAP is available. Click the notification to start the upgrade process.

Before you begin

Cloud Manager operations such as volume or aggregate creation must not be in progress for the Cloud Volumes ONTAP system.

Steps

1. Click **Canvas**.
2. Select a working environment.

A notification appears in the right pane if a new version is available:

The screenshot shows the Cloud Manager interface. At the top, there's a cloud icon and the text "Visual View". Below that, a card for "cloudvolumesontap1" is shown, indicating it's "On | AWS". The main area has two sections: "NOTIFICATIONS" and "SERVICES". The "NOTIFICATIONS" section has a red border around it and contains a message: "★ New version available". The "SERVICES" section contains a card for "Cloud Compliance" which is "On" and shows "No Personal Files Found".

3. If a new version is available, click **Upgrade**.
4. In the Release Information page, click the link to read the Release Notes for the specified version, and then select the **I have read...** check box.
5. In the End User License Agreement (EULA) page, read the EULA, and then select **I read and approve the EULA**.
6. In the Review and Approve page, read the important notes, select **I understand...**, and then click **Go**.

Result

Cloud Manager starts the software upgrade. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

Upgrading Cloud Volumes ONTAP by using an HTTP or FTP server

You can place the Cloud Volumes ONTAP software image on an HTTP or FTP server and then initiate the software upgrade from Cloud Manager. You might use this option if Cloud Manager can't access the S3 bucket to upgrade the software.

Steps

1. Set up an HTTP server or FTP server that can host the Cloud Volumes ONTAP software image.
2. If you have a VPN connection to the virtual network, you can place the Cloud Volumes ONTAP software image on an HTTP server or FTP server in your own network. Otherwise, you must place the file on an HTTP server or FTP server in the cloud.
3. If you use your own security group for Cloud Volumes ONTAP, ensure that the outbound rules allow HTTP or FTP connections so Cloud Volumes ONTAP can access the software image.



The predefined Cloud Volumes ONTAP security group allows outbound HTTP and FTP connections by default.

4. Obtain the software image from [the NetApp Support Site](#).
5. Copy the software image to the directory on the HTTP or FTP server from which the file will be served.
6. From the working environment in Cloud Manager, click the menu icon, and then click **Advanced > Update Cloud Volumes ONTAP**.
7. On the update software page, choose **Select an image available from a URL**, enter the URL, and then click **Change Image**.
8. Click **Proceed** to confirm.

Result

Cloud Manager starts the software update. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

Upgrading Cloud Volumes ONTAP by using a local image

Each Cloud Volumes ONTAP system can hold two software images: the current image that is running, and an alternate image that you can boot. Cloud Manager can change the alternate image to be the default image.

Steps

1. From the working environment, click the menu icon, and then click **Advanced > Update Cloud Volumes ONTAP**.
2. On the update software page, select the alternate image, and then click **Change Image**.
3. Click **Proceed** to confirm.

Result

Cloud Manager starts the software update. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

Modifying Cloud Volumes ONTAP systems

You might need to change the configuration of Cloud Volumes ONTAP systems as your storage needs change. For example, you can change between pay-as-you-go configurations, change the instance or VM type, and more.

Changing the instance or machine type for Cloud Volumes ONTAP

You can choose from several instance or machine types when you launch Cloud Volumes ONTAP in AWS, Azure, or GCP. You can change the instance or machine type at any time if you determine that it is undersized or oversized for your needs.

About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

[ONTAP 9 Documentation: Commands for configuring automatic giveback](#)

- Changing the instance or machine type affects cloud provider service charges.
- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

For HA pairs, the change is nondisruptive. HA pairs continue to serve data.



Cloud Manager gracefully changes one node at a time by initiating takeover and waiting for give back. NetApp's QA team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, we did see retries on the I/O level, but the application layer overcame these short "re-wire" of NFS/CIFS connections.

Steps

- From the working environment, click the menu icon, and then click **Change license or instance** for AWS, **Change license or VM** for Azure, or **Change license or machine** for GCP.
- If you are using a pay-as-you-go configuration, you can optionally choose a different license.
- Select an instance or machine type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

Result

Cloud Volumes ONTAP reboots with the new configuration.

Changing between hourly (pay-as-you-go) configurations

After you launch an hourly, pay-as-you-go Cloud Volumes ONTAP system, you can change between the Explore, Standard, and Premium configurations at any time by modifying the license. Changing the license increases or decreases the raw capacity limit and enables you to choose from different instance or VM types.

About this task

Note the following about changing between pay-as-you-go licenses:

- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

For HA pairs, the change is nondisruptive. HA pairs continue to serve data.

- Changing the instance or machine type affects cloud provider service charges.

Steps

- From the working environment, click the menu icon, and then click **Change license or instance** for AWS, **Change license or VM** for Azure, or **Change license or machine** for GCP.
- Select a license type and an instance type or machine type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

Result

Cloud Volumes ONTAP reboots with the new license, instance type or machine type, or both.

Moving to an alternate Cloud Volumes ONTAP configuration

If you want to switch between a pay-by-the-hour (PAYGO) subscription, an annual contract (AWS only), or a BYOL subscription, then you need to create a new Cloud Volumes ONTAP working environment and then replicate data from the existing working environment to the new working environment. The same is true if you want to switch between a single Cloud Volumes ONTAP system and an HA pair.

Steps

1. Create a new Cloud Volumes ONTAP working environment.

[Launching Cloud Volumes ONTAP in AWS](#)

[Launching Cloud Volumes ONTAP in Azure](#)

[Launching Cloud Volumes ONTAP in GCP](#)

2. [Set up one-time data replication](#) between the systems for each volume that you must replicate.
3. Terminate the Cloud Volumes ONTAP system that you no longer need by [deleting the original working environment](#).

Changing write speed to normal or high

Cloud Manager enables you to choose a normal or high write speed for Cloud Volumes ONTAP. The default write speed is normal. You can change to high write speed if fast write performance is required for your workload.

High write speed is supported with all types of single node systems. It's also supported with HA pairs in AWS and Azure when using a specific instance or VM type ([click here to see the list of supported instances and VM types](#)). High write speed is not supported with HA pairs in GCP.

Before you change the write speed, you should [understand the differences between the normal and high settings](#).

About this task

- Ensure that operations such as volume or aggregate creation are not in progress.
- Be aware that this change restarts Cloud Volumes ONTAP.

Steps

1. From the working environment, click the menu icon, and then click **Advanced > Writing Speed**.
2. Select **Normal** or **High**.

If you choose High, then you'll need to read the "I understand..." statement and confirm by checking the box.

3. Click **Save**, review the confirmation message, and then click **Proceed**.

Modifying the storage VM name

Cloud Manager automatically names the single storage VM (SVM) that it creates for Cloud Volumes ONTAP. You can modify the name of the SVM if you have strict naming standards. For example, you might want the name to match how you name the SVMs for your ONTAP clusters.

But if you created any additional SVMs for Cloud Volumes ONTAP, then you can't rename the SVMs from Cloud Manager. You'll need to do so directly from Cloud Volumes ONTAP by using System Manager or the CLI.

Steps

1. From the working environment, click the menu icon, and then click **Information**.
2. Click the edit icon to the right of the storage VM name.

The screenshot shows the 'Working Environment Information' page for an ONTAP system. The page displays various system details:

- Serial Number: [REDACTED]
- System ID: system-id-capacitytest
- Cluster Name: capacitytest
- ONTAP Version: 9.7RC1
- Date Created: Jul 6, 2020 07:42:02 am
- Storage VM Name: svm_capacitytest

3. In the Modify SVM Name dialog box, change the name, and then click **Save**.

Changing the password for Cloud Volumes ONTAP

Cloud Volumes ONTAP includes a cluster admin account. You can change the password for this account from Cloud Manager, if needed.



You should not change the password for the admin account through System Manager or the CLI. The password will not be reflected in Cloud Manager. As a result, Cloud Manager cannot monitor the instance properly.

Steps

1. From the working environment, click the menu icon, and then click **Advanced > Set password**.
2. Enter the new password twice and then click **Save**.

The new password must be different than one of the last six passwords that you used.

Changing route tables associated with HA pairs in multiple AWS AZs

You can modify the AWS route tables that include routes to the floating IP addresses for an HA pair. You might do this if new NFS or CIFS clients need to access an HA pair in AWS.

Steps

1. From the working environment, click the menu icon and then click **Information**.
2. Click **Route Tables**.
3. Modify the list of selected route tables and then click **Save**.

Result

Cloud Manager sends an AWS request to modify the route tables.

Managing the state of Cloud Volumes ONTAP

You can stop and start Cloud Volumes ONTAP from Cloud Manager to manage your cloud compute costs.

Scheduling automatic shutdowns of Cloud Volumes ONTAP

You might want to shut down Cloud Volumes ONTAP during specific time intervals to lower your compute costs. Rather than do this manually, you can configure Cloud Manager to automatically shut down and then restart systems at specific times.

About this task

- When you schedule an automatic shutdown of your Cloud Volumes ONTAP system, Cloud Manager postpones the shutdown if an active data transfer is in progress.

Cloud Manager shuts down the system after the transfer is complete.

- This task schedules automatic shutdowns of both nodes in an HA pair.
- Snapshots of boot and root disks are not created when turning off Cloud Volumes ONTAP through scheduled shutdowns.

Snapshots are automatically created only when performing a manual shutdown, as described in the next section.

Steps

1. From the working environment, click the clock icon:



2. Specify the shutdown schedule:

- a. Choose whether you want to shut down the system every day, every weekday, every weekend, or any combination of the three options.
- b. Specify when you want to turn off the system and for how long you want it turned off.

Example

The following image shows a schedule that instructs Cloud Manager to shut down the system every

Saturday at 12:00 a.m. for 48 hours. Cloud Manager restarts the system every Monday at 12:00 a.m.

<input type="checkbox"/> Turn off every weekday	turn off at	08	:	00	PM	for	12	Hours (1-24)
Mon, Tue, Wed, Thu, Fri								
<input checked="" type="checkbox"/> Turn off every weekend	turn off at	12	:	00	AM	for	48	Hours (1-48)
Sat								

3. Click **Save**.

Result

Cloud Manager saves the schedule. The clock icon changes to indicate that a schedule is set:



Stopping Cloud Volumes ONTAP

Stopping Cloud Volumes ONTAP saves you from accruing compute costs and creates snapshots of the root and boot disks, which can be helpful for troubleshooting.



To reduce costs, Cloud Manager periodically deletes older snapshots of root and boot disks. Only the two most recent snapshots are retained for both the root and boot disks.

About this task

When you stop an HA pair, Cloud Manager shuts down both nodes.

Steps

1. From the working environment, click the **Turn off** icon.



2. Keep the option to create snapshots enabled because the snapshots can enable system recovery.

3. Click **Turn Off**.

It can take up to a few minutes to stop the system. You can restart systems at a later time from the working environment page.

Monitoring AWS resource costs

Cloud Manager enables you to view the resource costs associated with running Cloud Volumes ONTAP in AWS. You can also see how much money you saved by using NetApp features that can reduce storage costs.

About this task

Cloud Manager updates the costs when you refresh the page. You should refer to AWS for final cost details.

Step

1. Verify that Cloud Manager can obtain cost information from AWS:
 - a. Ensure that the IAM policy that provides Cloud Manager with permissions includes the following actions:

```
"ce:GetReservationUtilization",
"ce:GetDimensionValues",
"ce:GetCostAndUsage",
"ce:GetTags"
```

These actions are included in the latest [Cloud Manager policy](#). New systems deployed from NetApp Cloud Central automatically include these permissions.

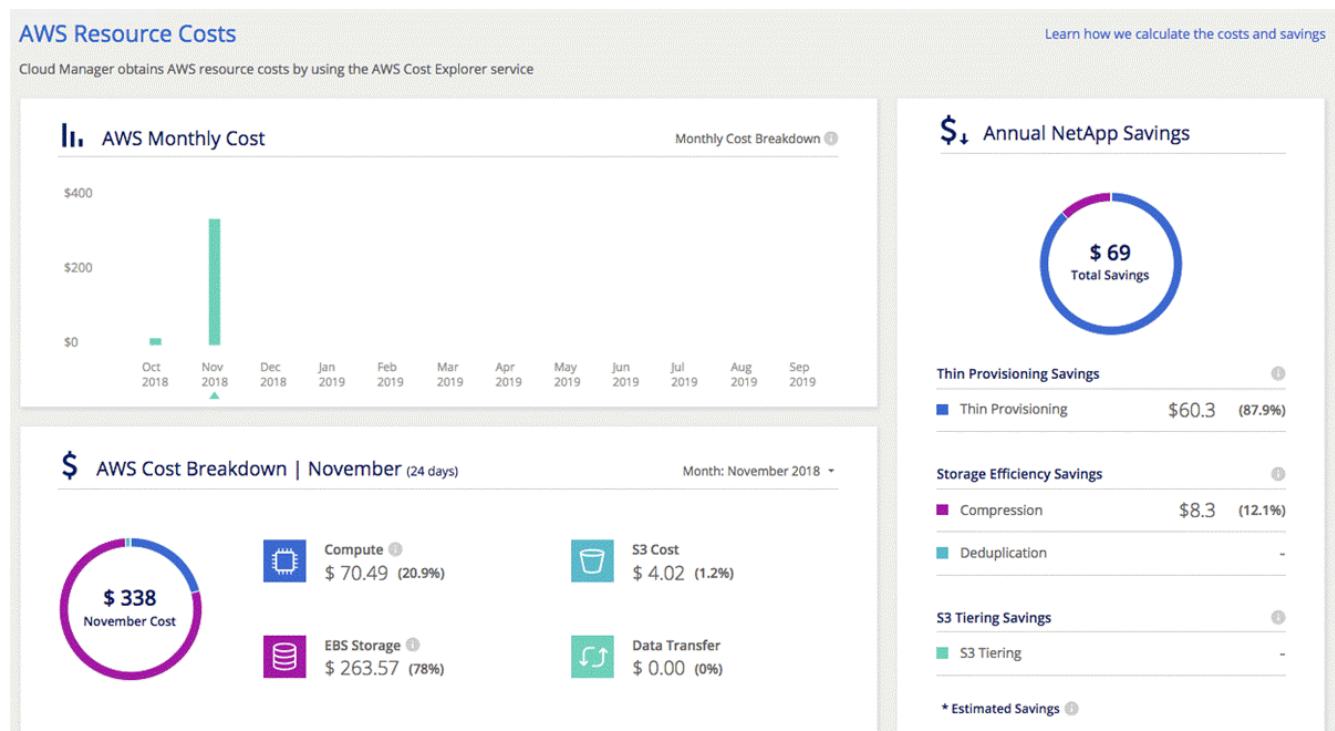
- b. [Activate the WorkingEnvironmentId tag](#).

To track your AWS costs, Cloud Manager assigns a cost allocation tag to Cloud Volumes ONTAP instances. After you create your first working environment, activate the **WorkingEnvironmentId** tag. User-defined tags don't appear on AWS billing reports until you activate them in the Billing and Cost Management console.

2. On the Canvas page, select a Cloud Volumes ONTAP working environment and then click **Cost**.

The Cost page displays costs for the current and previous months and shows your annual NetApp savings, if you enabled NetApp's cost-saving features on volumes.

The following image shows a sample Cost page:



Connecting to Cloud Volumes ONTAP

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using OnCommand System Manager or the command line interface.

Connecting to System Manager

You might need to perform some Cloud Volumes ONTAP tasks from System Manager, which is a browser-based management tool that runs on the Cloud Volumes ONTAP system. For example, you need to use System Manager if you want to create LUNs.

Before you begin

The computer from which you are accessing Cloud Manager must have a network connection to Cloud Volumes ONTAP. For example, you might need to log in to Cloud Manager from a jump host that's in your cloud provider network.



When deployed in multiple AWS Availability Zones, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

Steps

1. From the Canvas page, double-click the Cloud Volumes ONTAP system that you want to manage with System Manager.
2. Click the menu icon, and then click **Advanced > System Manager**.
3. Click **Launch**.

System Manager loads in a new browser tab.

4. At the login screen, enter **admin** in the User Name field, enter the password that you specified when you created the working environment, and then click **Sign In**.

Result

The System Manager console loads. You can now use it to manage Cloud Volumes ONTAP.

Connecting to the Cloud Volumes ONTAP CLI

The Cloud Volumes ONTAP CLI enables you to run all administrative commands and is a good choice for advanced tasks or if you are more comfortable using the CLI. You can connect to the CLI using Secure Shell (SSH).

Before you begin

The host from which you use SSH to connect to Cloud Volumes ONTAP must have a network connection to Cloud Volumes ONTAP. For example, you might need to use SSH from a jump host in AWS or Azure.



When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

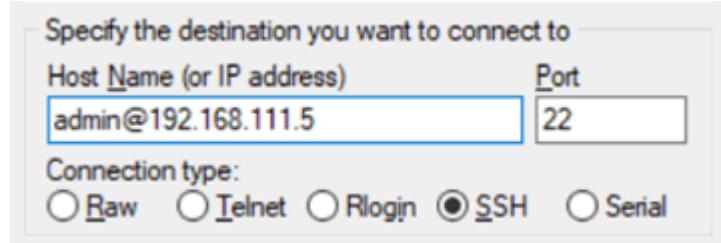
Steps

1. In Cloud Manager, identify the IP address of the cluster management interface:

- a. On the Canvas page, select the Cloud Volumes ONTAP system.
 - b. Copy the cluster management IP address that appears in the right pane.
2. Use SSH to connect to the cluster management interface IP address using the admin account.

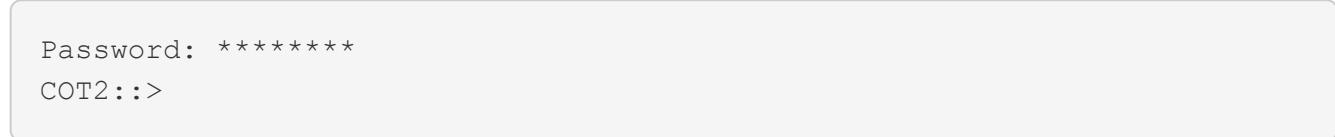
Example

The following image shows an example using PuTTY:



3. At the login prompt, enter the password for the admin account.

Example



Adding existing Cloud Volumes ONTAP systems to Cloud Manager

You can discover and add existing Cloud Volumes ONTAP systems to Cloud Manager. You might do this if you deployed a new Cloud Manager system.

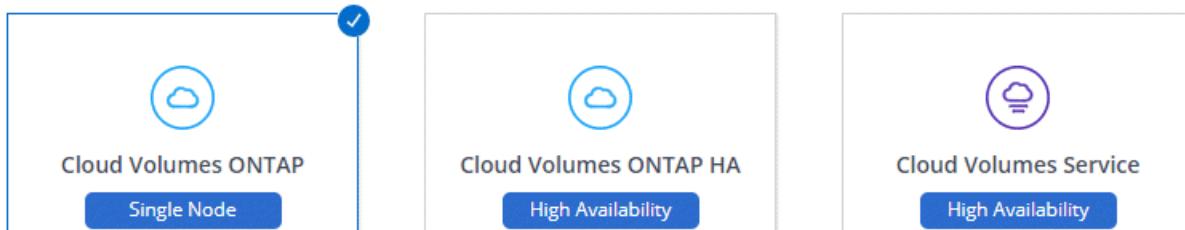
Before you begin

You must know the password for the Cloud Volumes ONTAP admin user account.

Steps

1. On the Canvas page, click **Add Working Environment**.
2. Select the cloud provider in which the system resides.
3. Choose the type of Cloud Volumes ONTAP system.
4. Click the link to discover an existing system.

Define Your Working Environment



[Learn More](#)

[Learn More](#)

[Learn More](#)

You're about to create a new **Cloud Volumes ONTAP** system in AWS.

 If you want to discover an existing Cloud Volumes ONTAP in AWS, [click here](#).

5. On the Region page, choose the region where the instances are running, and then select the instances.
6. On the Credentials page, enter the password for the Cloud Volumes ONTAP admin user, and then click **Go**.

Result

Cloud Manager adds the Cloud Volumes ONTAP instances to the workspace.

Overriding CIFS locks for Cloud Volumes ONTAP HA in Azure

The Account Admin can enable a setting in Cloud Manager that prevents issues with Cloud Volumes ONTAP storage failover during Azure maintenance events. When you enable this setting, Cloud Volumes ONTAP vetoes CIFS locks and resets active CIFS sessions.

About this task

Microsoft Azure schedules periodic maintenance events on its virtual machines. When a maintenance event occurs on a node in a Cloud Volumes ONTAP HA pair, the HA pair initiates storage takeover. If there are active CIFS sessions during this maintenance event, the locks on CIFS files can prevent storage failover.

If you enable this setting, Cloud Volumes ONTAP will veto the locks and reset the active CIFS sessions. As a result, the HA pair can complete storage failover during these maintenance events.



This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

What you'll need

You need to create a Connector before you can change Cloud Manager settings. [Learn how](#).

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.



2. Under **Azure**, click **Azure CIFS locks for Azure HA working environments**.

3. Click the checkbox to enable the feature and then click **Save**.

Using an Azure Private Link with Cloud Volumes ONTAP

By default, Cloud Manager enables an Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts. A Private Link secures connections between endpoints in Azure and provides performance benefits. [Learn more](#).

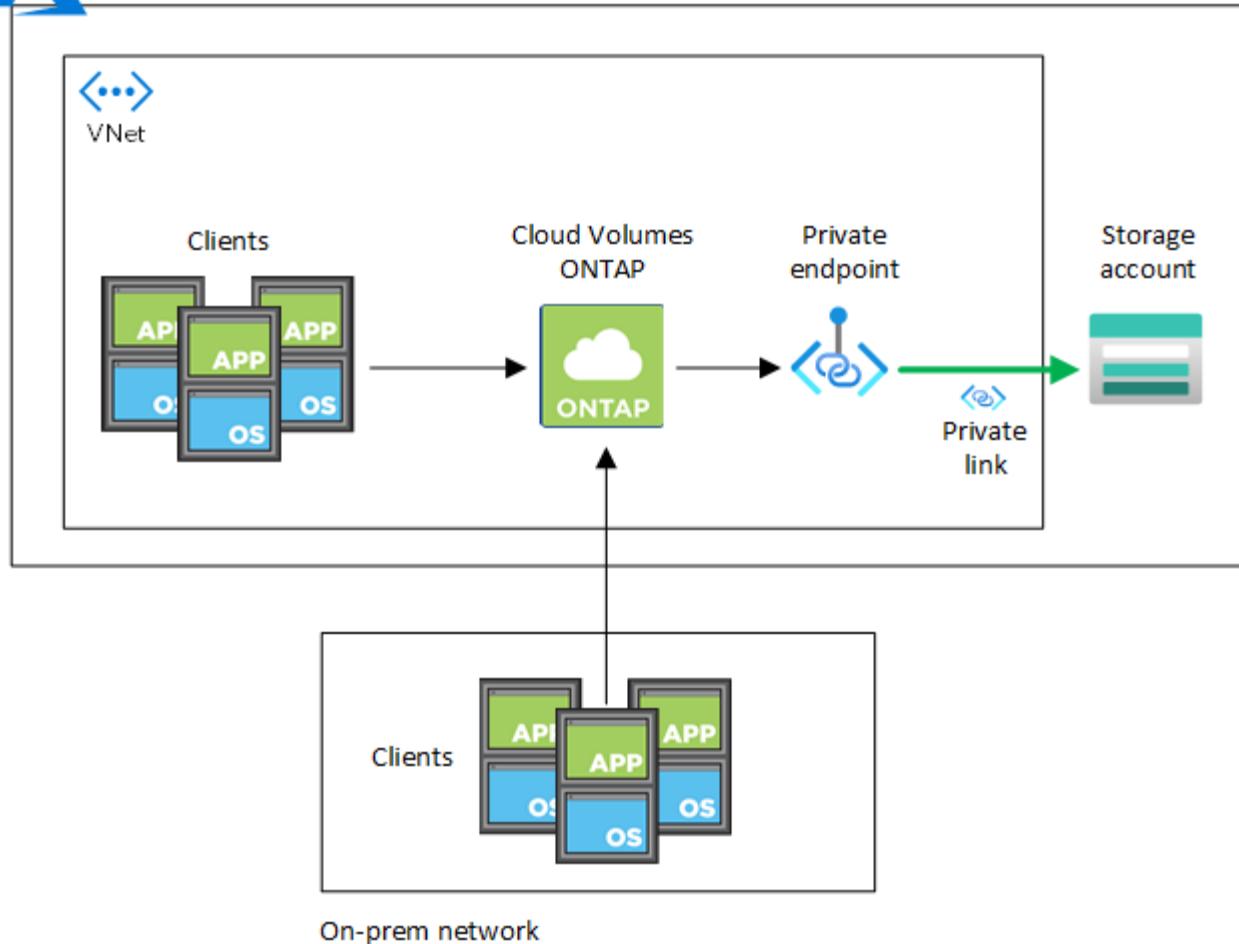
In most cases, there's nothing that you need to do—Cloud Manager manages the Azure Private Link for you. But if you use Azure Private DNS, then you'll need to edit a configuration file. You can also disable the Private Link connection, if desired.

How Private Link connections work with Cloud Volumes ONTAP

When Cloud Manager deploys Cloud Volumes ONTAP in Azure, it creates a private endpoint in the resource group. The private endpoint is associated with the storage account for Cloud Volumes ONTAP. As a result, access to Cloud Volumes ONTAP storage travels through the Microsoft backbone network.

Client access goes through the private link when clients are within the same VNet as Cloud Volumes ONTAP, within peered VNets, or in your on-premises network when using a private VPN or ExpressRoute connection to the VNet.

Here's an example that shows client access over a private link from within the same VNet and from an on-prem network that has either a private VPN or ExpressRoute connection.



Providing Cloud Manager with details about your Azure Private DNS

If you use [Azure Private DNS](#), then you need to modify a configuration file on each Connector. Otherwise, Cloud Manager can't enable the Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts.

Note that the DNS name must match Azure DNS naming requirements as shown in [Azure documentation](#).

Steps

1. SSH to the Connector host and log in.
2. Navigate to the following directory: /opt/application/netapp/cloudmanager/docker_occm/data
3. Edit app.conf by modifying the following parameter as shown:

```
"user-private-dns-zone-settings": {  
    "use-existing": true,  
    "resource-group": "<resource group name of the DNS zone>"  
}
```

4. Save the file and log off the Connector.

A reboot isn't required.

Disabling Azure Private Link connections

If required for your Azure configuration, you can disable the Azure Private Link connection between Cloud Volumes ONTAP and storage accounts.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.
2. Under **Azure**, click **Use Azure Private Link**.
3. Deselect **Private Link connection between Cloud Volumes ONTAP and storage accounts**.
4. Click **Save**.

Deleting a Cloud Volumes ONTAP working environment

You should always delete Cloud Volumes ONTAP systems from Cloud Manager, rather than from your cloud provider's console. For example, if you terminate a licensed Cloud Volumes ONTAP instance from your cloud provider, then you can't use the license key for another instance. You must delete the working environment from Cloud Manager to release the license.

When you delete a working environment, Cloud Manager terminates Cloud Volumes ONTAP instances and deletes disks and snapshots.

Resources managed by other services like backups for Cloud Backup and instances for Cloud Data Sense and Monitoring are not deleted when you delete a working environment. You'll need to manually delete them yourself. If you don't, then you'll continue to receive charges for these resources.



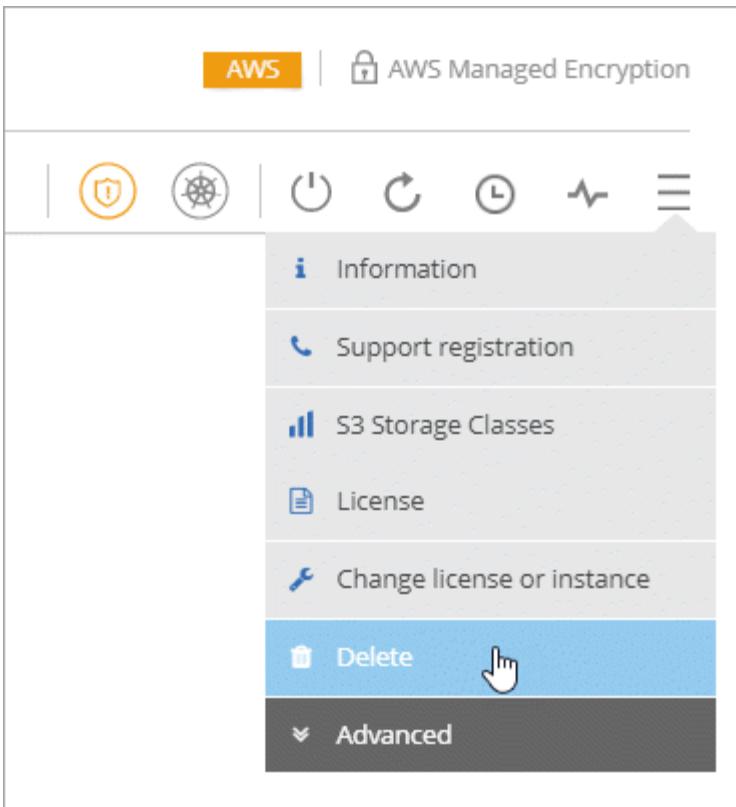
When Cloud Manager deploys Cloud Volumes ONTAP in your cloud provider, it enables termination protection on the instances. This option helps prevent accidental termination.

Steps

1. If you enabled Cloud Backup on the working environment, determine whether the backed up data is still required and then [delete the backups, if necessary](#).

Cloud Backup is independent from Cloud Volumes ONTAP by design. Cloud Backup doesn't automatically delete backups when you delete a Cloud Volumes ONTAP system, and there is no current support in the UI to delete the backups after the system has been deleted.

2. If you enabled Cloud Data Sense or Monitoring on this working environment and no other working environments use those services, then you'll need to delete the instances for those services.
 - [Learn more about the Cloud Data Sense instance](#).
 - [Learn more about the Monitoring Acquisition Unit](#).
3. Delete the Cloud Volumes ONTAP working environment.
 - a. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment that you want to delete.
 - b. Click menu icon and then click **Delete**.



- c. Type the name of the working environment and then click **Delete**.

It can take up to 5 minutes to delete the working environment.

Copyright Information

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

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

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

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

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

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

Trademark Information

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