Learn

Cloud Manager

NetApp
October 11, 2021

Table of Contents

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

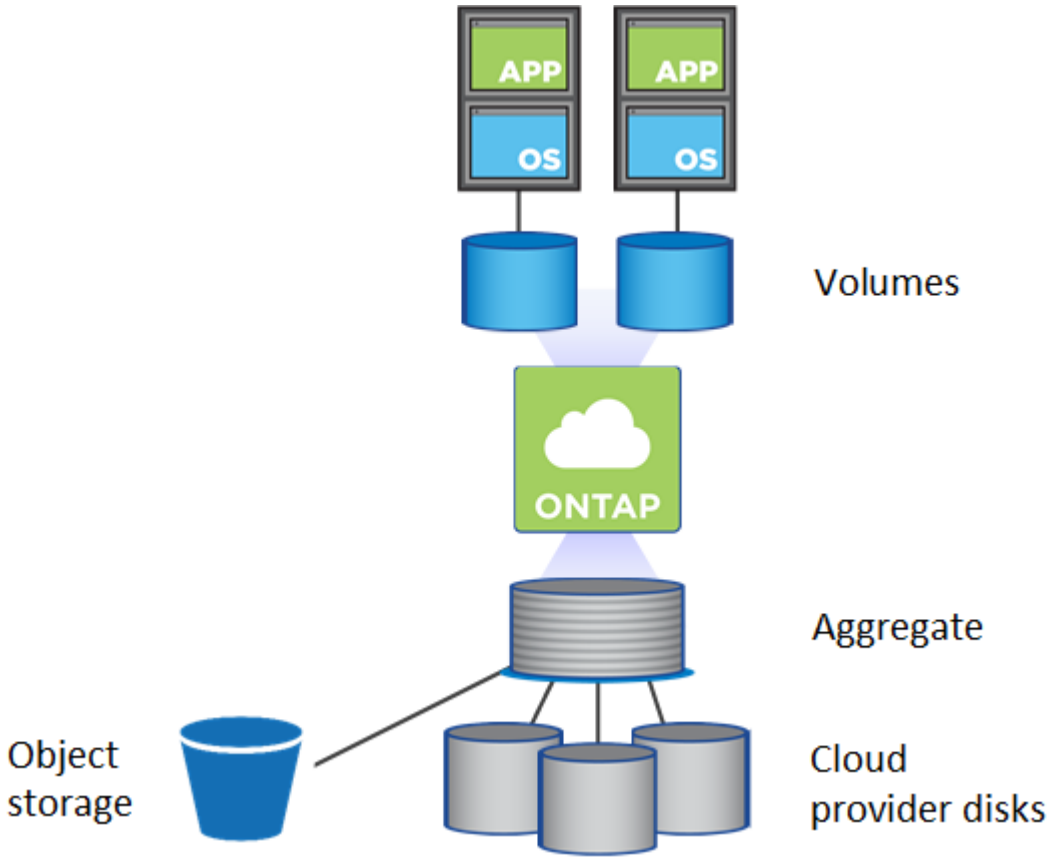
Disks and aggregates

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 GiB aggregate, the usable capacity is 442.94 GiB.

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 TiB.

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 TiB.

  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 TiB.

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 TiB.

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

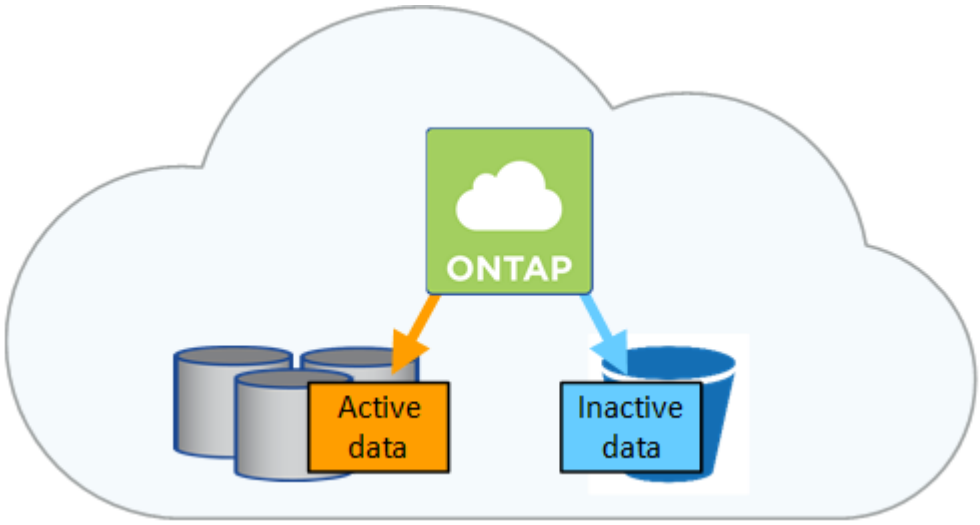
- Google Cloud Platform documentation: Storage Options
- Review storage limits for Cloud Volumes ONTAP in GCP

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 SSD persistent disks, balanced persistent disks, or standard persistent 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 GiB	3 TiB
4	1 TiB	6 TiB

Aggregate number	Disk size	Max aggregate capacity
6	2 TiB	12 TiB

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.

  Cloud Manager checks the free space ratio every 15 minutes to determine if it needs to purchase additional disks.

- 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.

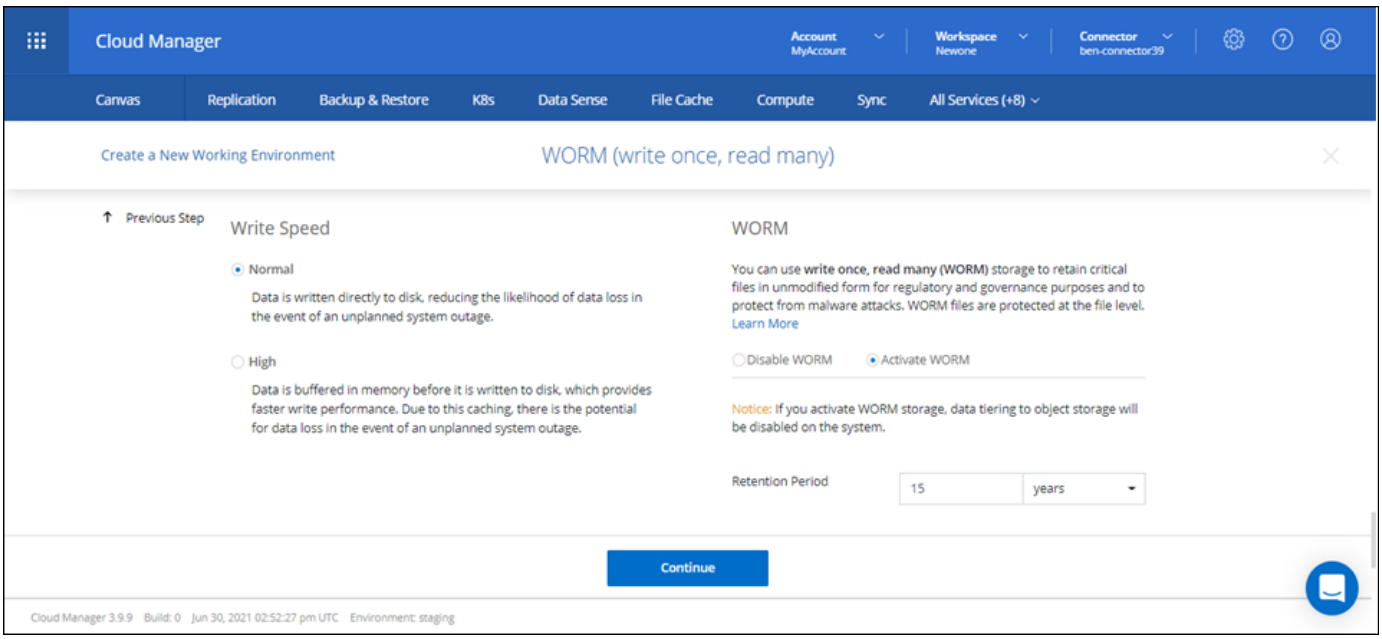
After the retention period has elapsed, you are responsible for deleting any files that you no longer need.

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:



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 GiB.

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.

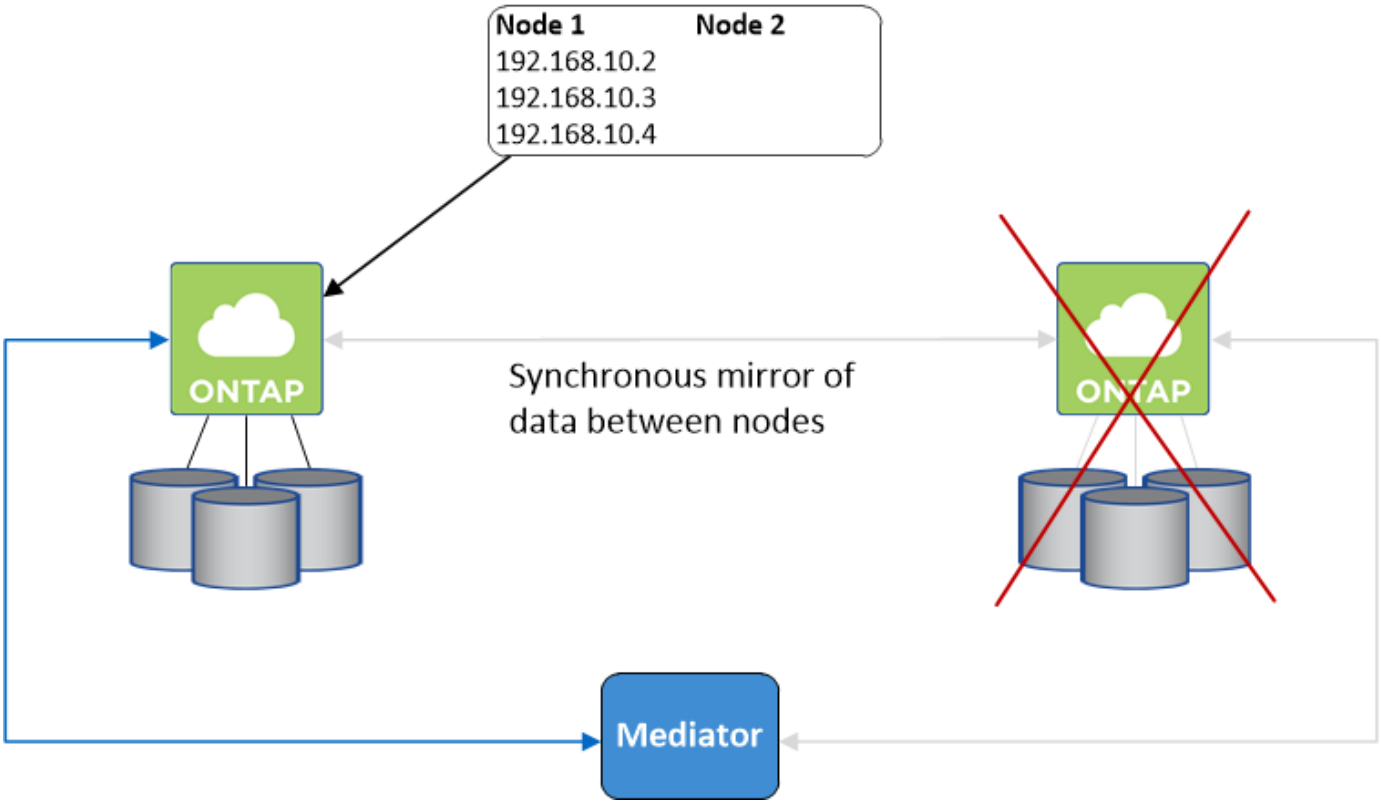
Takeover and giveback for iSCSI

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

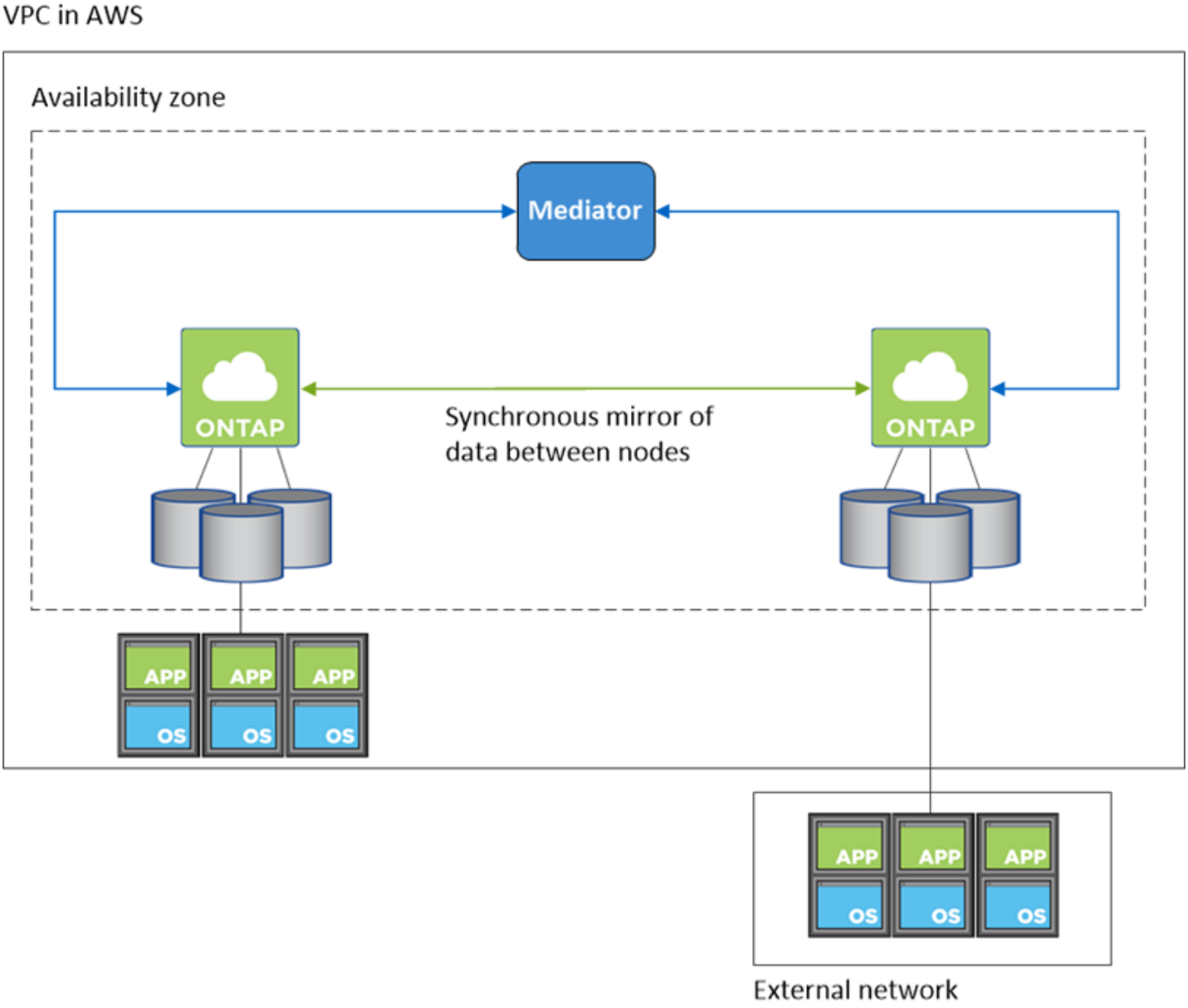
Deploying an HA configuration in a single Availability Zone (AZ) can ensure high availability of your data if an instance that runs a Cloud Volumes ONTAP node fails. All data is natively accessible from outside of the VPC.

> 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.



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.

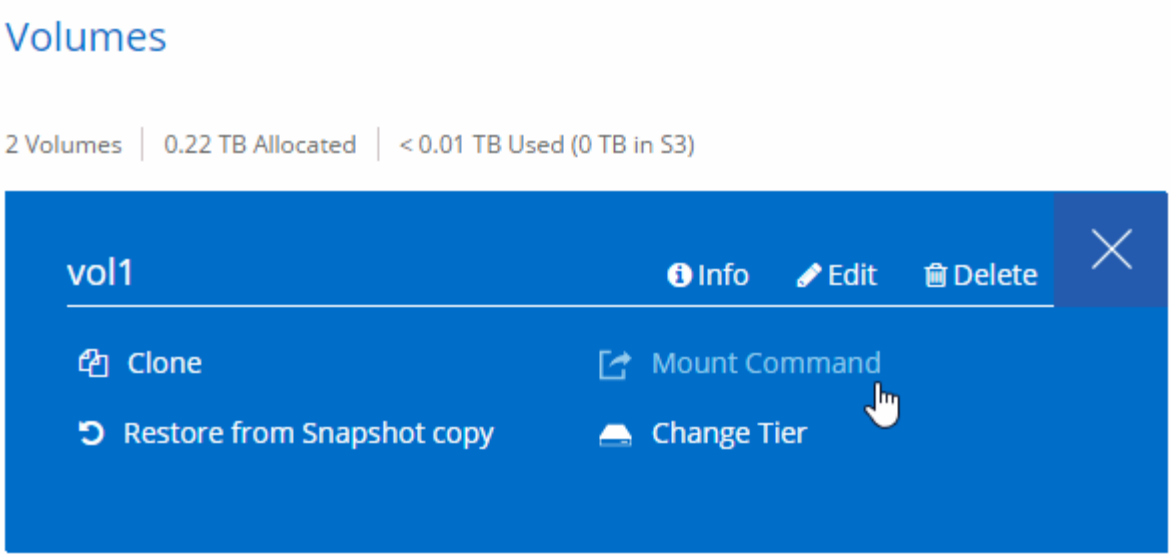
For more details about Cloud Volumes ONTAP performance, see Performance.

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:

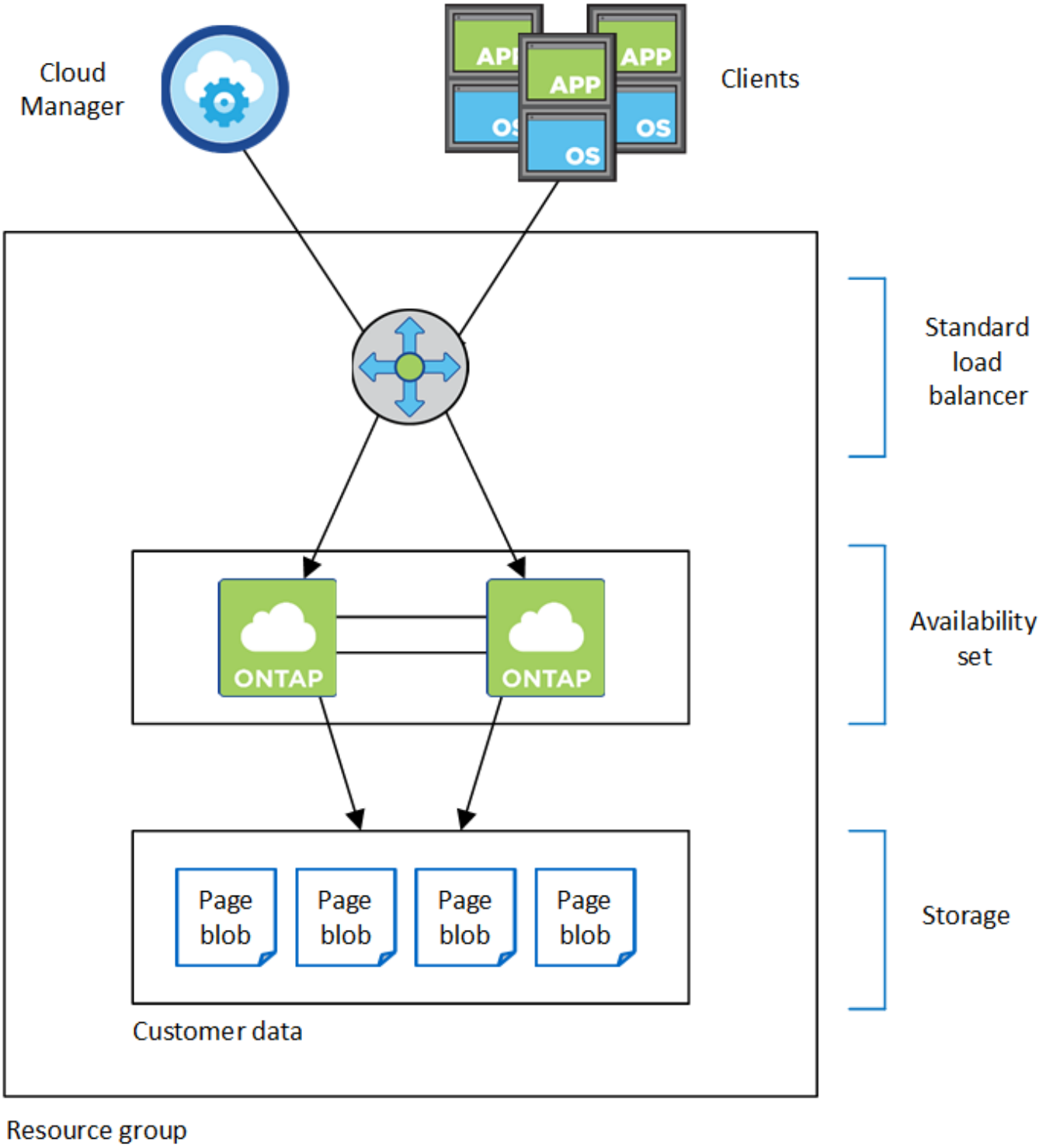


High-availability pairs in Azure

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:



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.

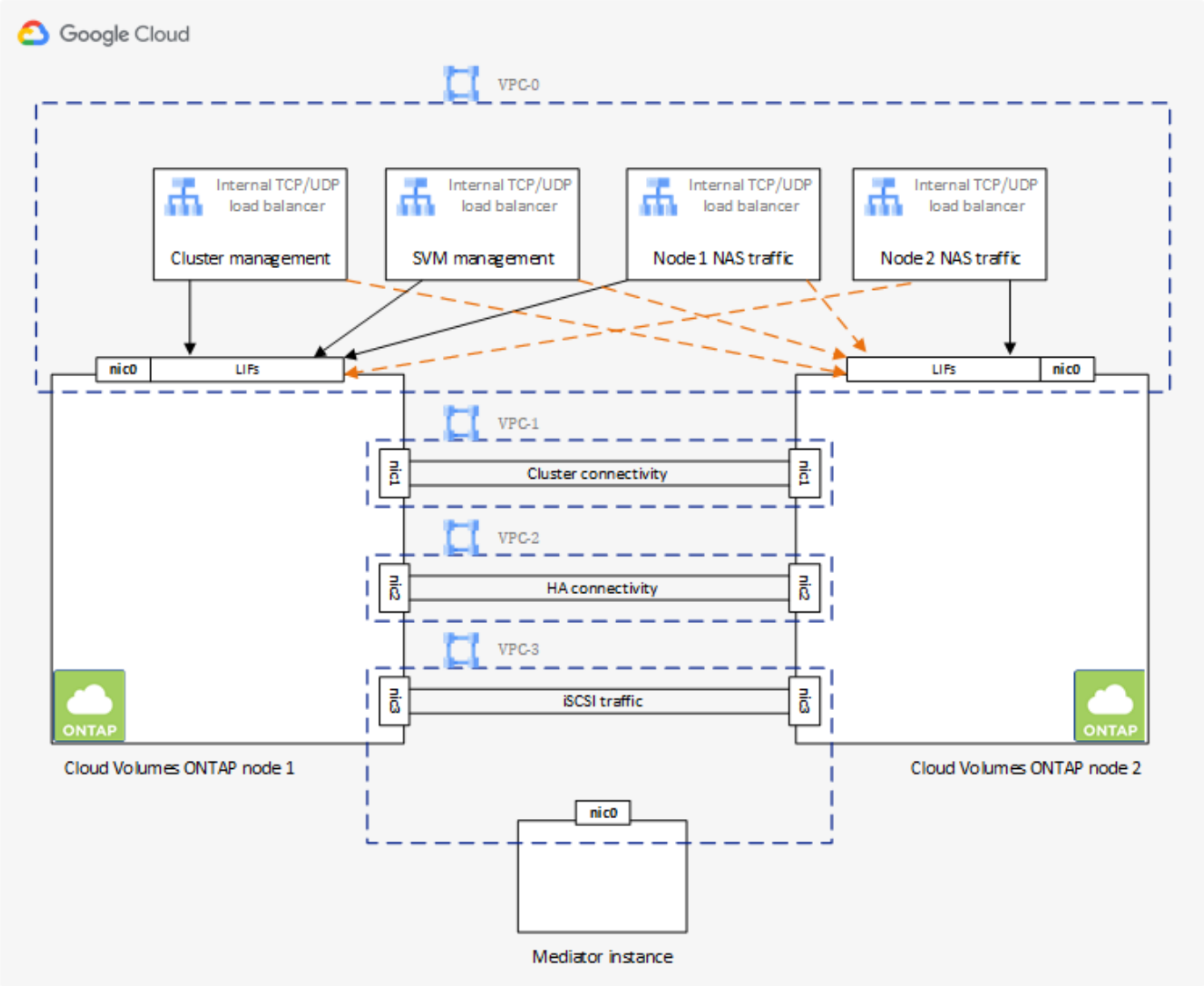
- Four Virtual Private Clouds (VPCs).

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

- Four Google Cloud internal load balancers (TCP/UDP) that manage incoming traffic to the Cloud Volumes ONTAP HA pair.

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.

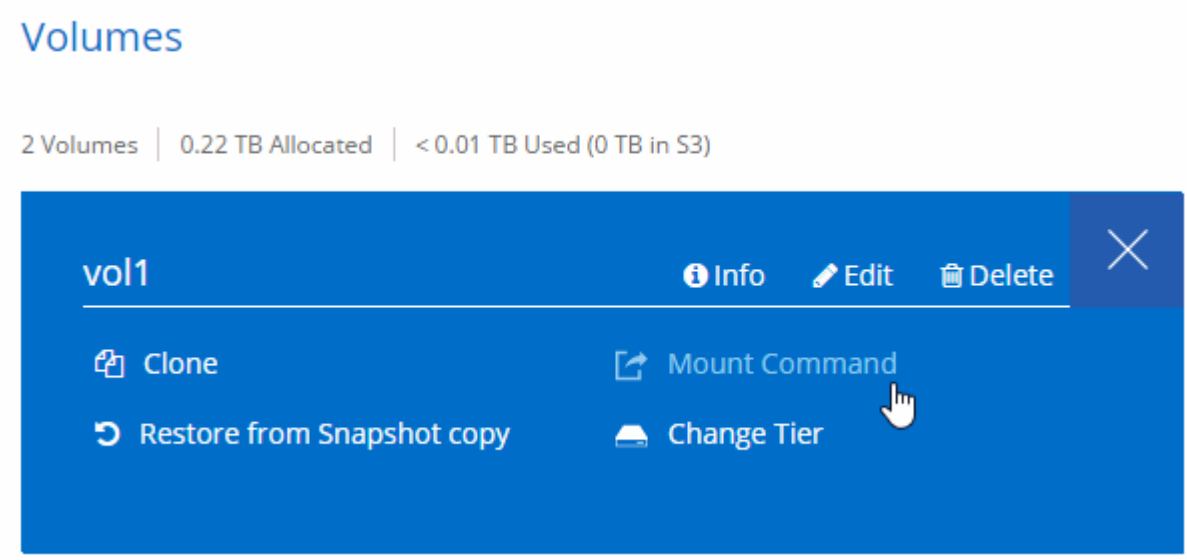
For more details about Cloud Volumes ONTAP performance, see Performance.

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:



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	• Pay per TiB of capacity for one or more Cloud Volumes ONTAP systems • Provides a la carte licensing for Cloud Volumes ONTAP: ◦ 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	• 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	• 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	• Explore: 2 TiB • Standard: 10 TiB • Premium: 368 TiB
Node-based license	• The previous generation BYOL for Cloud Volumes ONTAP • A node-based license is available for license renewals only	Included	368 TiB 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 GiB 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 GiB, 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 GiB 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 TiB license, deploy four Cloud Volumes ONTAP systems, and then allocate a 5 TiB volume to each system, for a total of 20 TiB.

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 TiB capacity charge. Any Cloud Volumes ONTAP instance that has less than 4 TiB of capacity will be charged at a rate of 4 TiB.

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

- The previous generation BYOL for Cloud Volumes ONTAP.
- A node-based license is available for license renewals only.
- Each Cloud Volumes ONTAP system supports up to 368 TiB 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.

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 TiB 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 TiB of capacity. For example, you might purchase two licenses to allocate up to 736 TiB 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

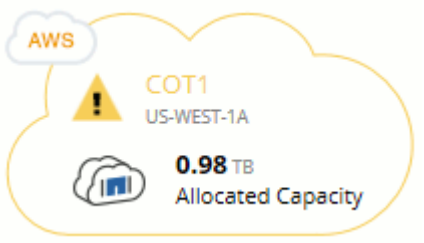
When you create a node-based BYOL system, Cloud Manager prompts you for the serial number of your license and your NetApp Support Site account. Cloud Manager uses the account to download the license file from NetApp and to install it on the Cloud Volumes ONTAP system.

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.

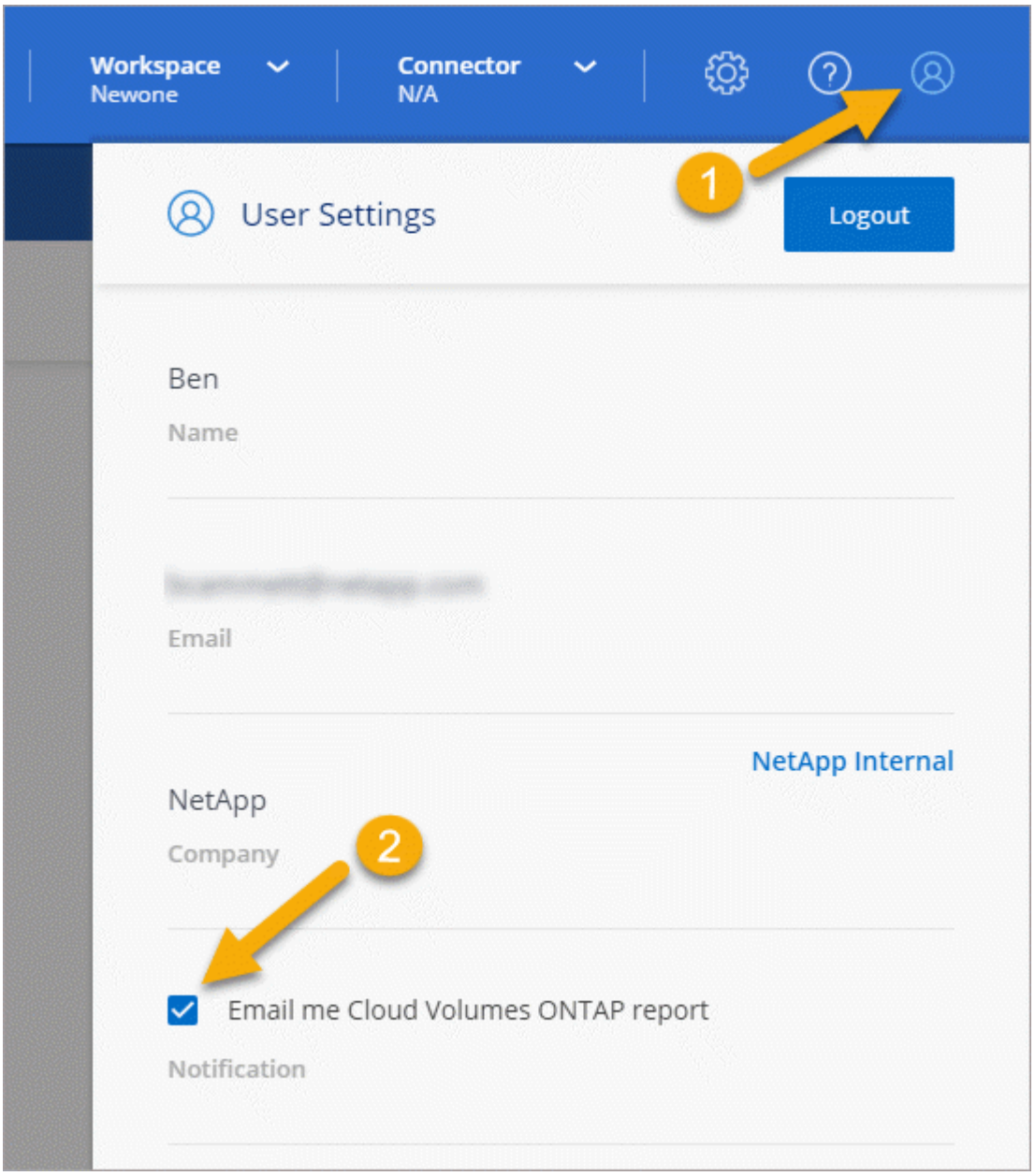
License expiration

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 GiB 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 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.

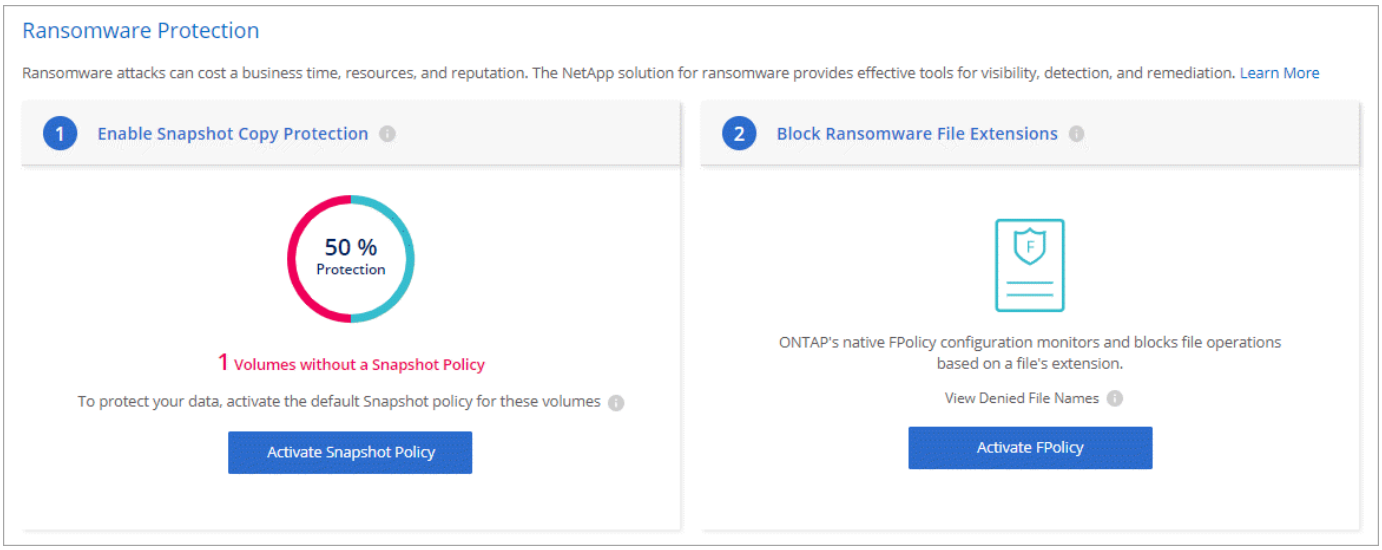
Ransomware protection

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.



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 The Account Admin can modify this value from the Settings page.
Security style	NTFS for CIFS volumes UNIX for NFS volumes

Attribute	Value set by Cloud Manager
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 GiB io1 disk for boot data and a 220 GiB gp2 disk for root data
  - 9.6: 93 GiB io1 disk for boot data and a 140 GiB gp2 disk for root data
  - 9.5: 45 GiB io1 disk for boot data and a 140 GiB gp2 disk for root data
- Starting with version 9.8, a 540 GiB 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 GiB

Azure (single node)

- Three Premium SSD disks:
  - One 10 GiB disk for boot data
  - One 140 GiB disk for root data
  - One 128 GiB 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 GiB Standard HDD disk for saving cores
- One Azure snapshot for each boot disk and root disk

Azure (HA pairs)

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

GCP

- One 10 GiB Standard persistent disk for boot data
- One 64 GiB Standard persistent disk for root data
- One 500 GiB Standard persistent disk for NVRAM
- One 315 GiB 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.