



Cloud & Manager 3.5

Concepts

NetApp Docs
2020

Table of Contents

1. Concepts	1
1.1. Cloud Manager and Cloud Volumes ONTAP overview	1
1.2. NetApp Cloud Central	2
1.3. Storage	3
1.4. Storage management	8
1.5. High-availability pairs	14
1.6. Security	19
1.7. WORM storage	19
1.8. Licensing	20
1.9. Performance	21
1.10. Cloud Storage Automation	21

1. Concepts

1.1. Cloud Manager and Cloud Volumes ONTAP overview

OnCommand Cloud Manager enables you to deploy Cloud Volumes ONTAP, which provides enterprise-class features for your cloud storage, and to easily replicate data across hybrid clouds built on NetApp.

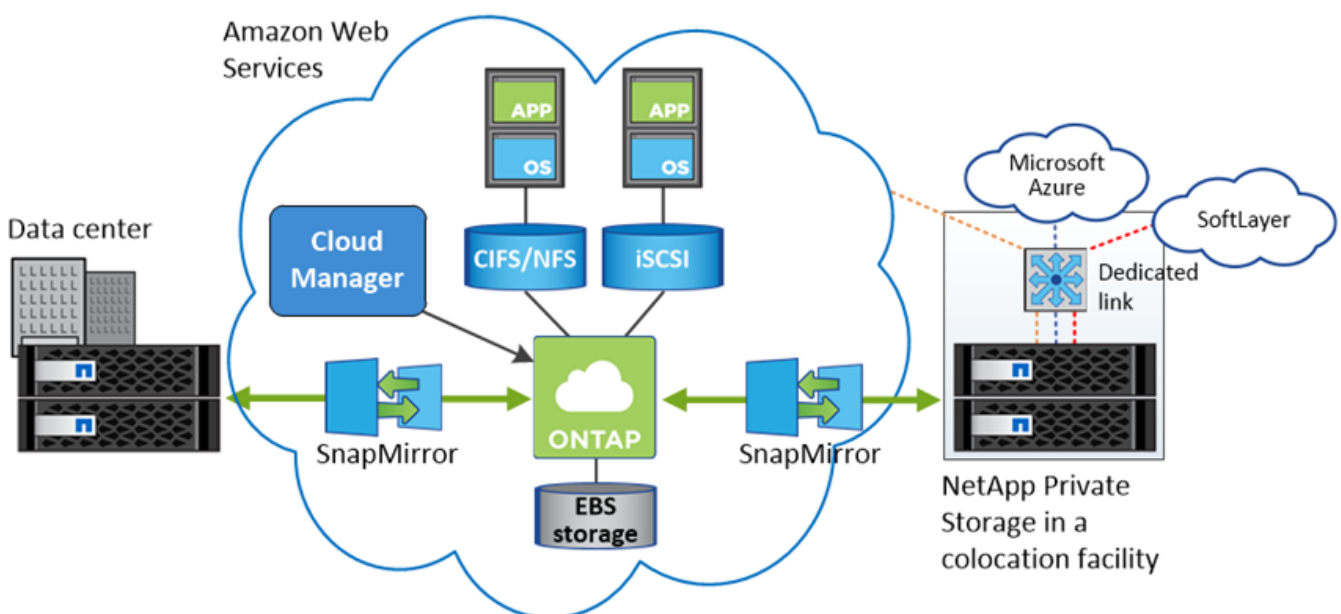
1.1.1. Cloud Manager

Cloud Manager was built with simplicity in mind. It guides you through Cloud Volumes ONTAP setup in a few quick steps, eases data management by offering simplified storage provisioning and automated capacity management, enables drag-and-drop data replication across a hybrid cloud, and more.

Cloud Manager is required to deploy and manage Cloud Volumes ONTAP, but it can also discover and provision storage for on-premises ONTAP clusters. This provides a central point of control for your cloud and on-premises storage infrastructure.

Cloud Manager also offers insight into your AWS cloud storage. The Cloud Storage Automation feature analyzes your cloud storage to show you savings opportunities, data protection enhancements, and operations that can optimize the cloud storage associated with your AWS account.

You can run Cloud Manager in the cloud or in your network—it just needs a connection to the networks in which you want to deploy Cloud Volumes ONTAP. The following image shows Cloud Manager running in AWS and managing Cloud Volumes ONTAP systems in AWS and Azure. It also shows data replication across a hybrid cloud.



[Learn more about Cloud Manager](#)

1.1.2. Cloud Volumes ONTAP

Cloud Volumes ONTAP is a software-only storage appliance that runs the ONTAP data management software in the cloud. You can use Cloud Volumes ONTAP for production workloads, disaster recovery, DevOps, file shares, and database management.

Cloud Volumes ONTAP extends enterprise storage to the cloud 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 (AWS only).
- **Data replication**
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.
- **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 the NetApp SnapManager tool suite.



Licenses for ONTAP features are included with Cloud Volumes ONTAP.

[View supported Cloud Volumes ONTAP configurations](#)

[Learn more about Cloud Volumes ONTAP](#)

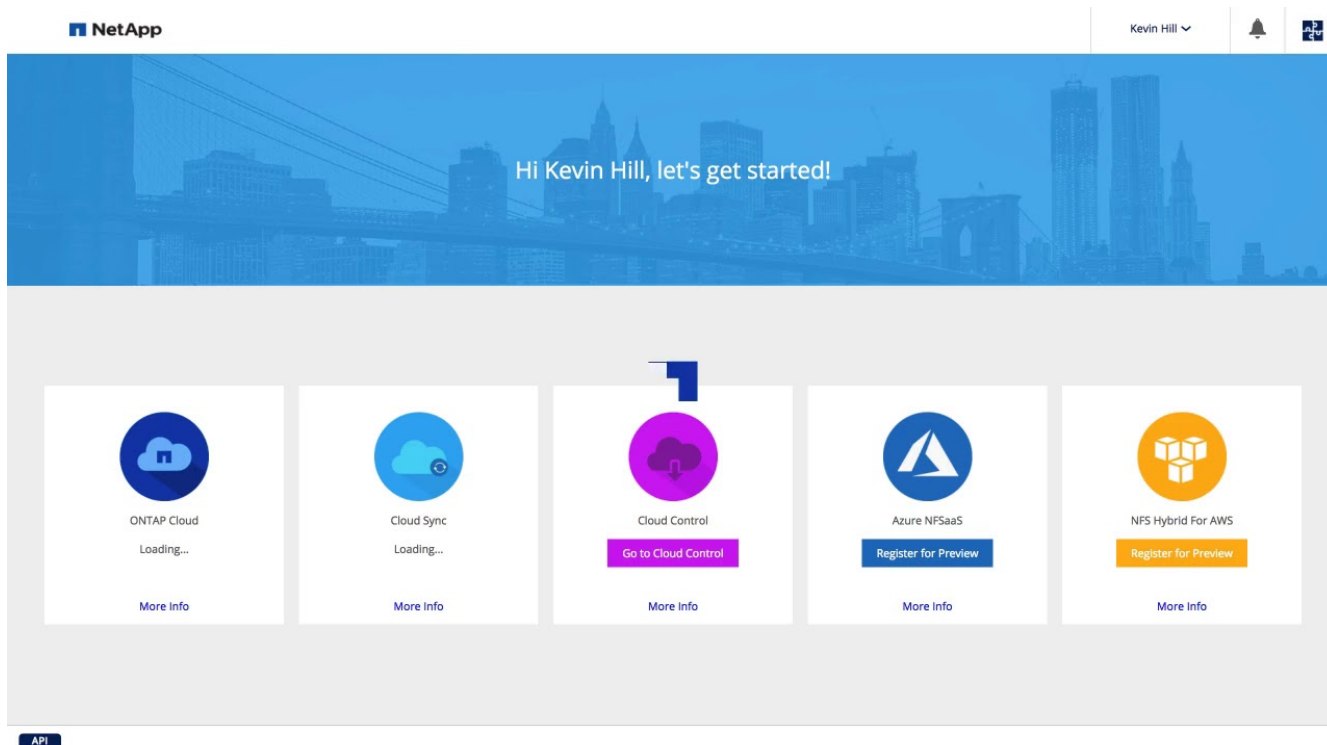
1.2. NetApp Cloud Central

[NetApp Cloud Central](#) provides a centralized location to access and manage NetApp cloud data services. These services enable you to run critical applications in the cloud, create automated DR sites, back up your SaaS data, and effectively migrate and control data across multiple clouds.

Cloud Manager's integration with NetApp Cloud Central provides several benefits, including a simplified deployment experience, a single location to view and manage multiple Cloud Manager systems, and centralized user authentication.

With centralized user authentication, you can use the same set of credentials across Cloud Manager systems and between Cloud Manager and other data services, such as Cloud Sync. It's also easy to reset your password if you forgot it.

The following video provides an overview of NetApp Cloud Central:

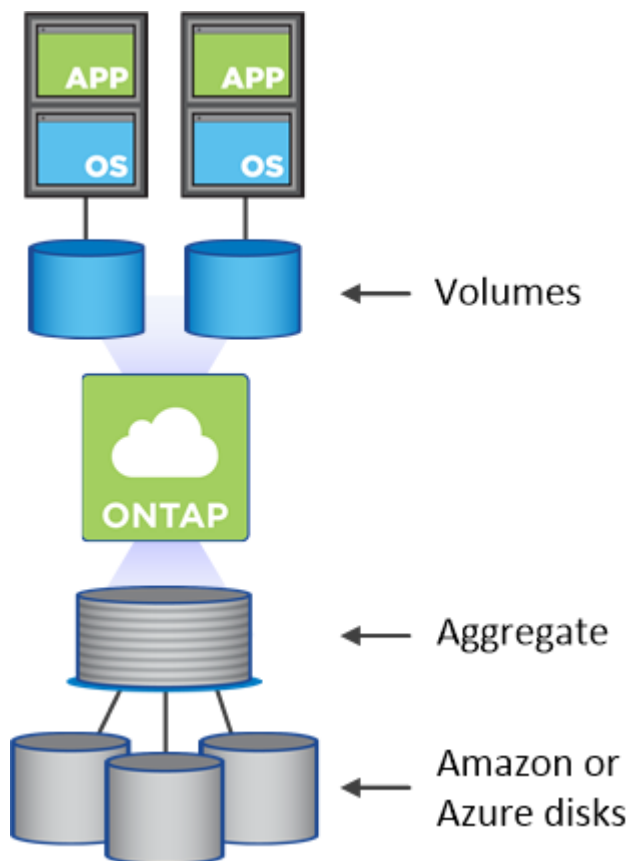


1.3. Storage

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

1.3.1. How Cloud Volumes ONTAP uses cloud storage

Cloud Volumes ONTAP uses AWS and Azure volumes as back-end storage. It sees these volumes as disks and groups them into one or more aggregates. Aggregates provide storage to one or more volumes.



In AWS, an aggregate can contain up to 6 disks, with a maximum disk size of 16 TB. The underlying EBS disk type can be either General Purpose SSD, Provisioned IOPS SSD, Throughput Optimized HDD, or Cold HDD. You can also pair an EBS disk with Amazon S3 for [data tiering](#) (not supported with Cold HDDs).

In Azure, an aggregate can contain up to 12 disks, with a maximum disk size of 4 TB. The underlying Azure managed disk type can be either Standard Storage (HDD) or Premium Storage (SSD). You can also pair a managed disk with Azure Blob storage for [data tiering](#).

You choose the disk type when creating volumes and the default disk size when you deploy Cloud Volumes ONTAP. For more details, refer to the following:

- [Choosing an AWS disk type](#)
- [Choosing an Azure disk type](#)
- [Choosing a disk size](#)



The total amount of storage purchased from AWS or Azure 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.

1.3.2. Data tiering overview

You can reduce your storage costs by enabling automated tiering of cold data to low-cost object storage. Active data remains in high-performance SSDs or HDDs (the performance tier), while inactive data is tiered to low-cost object storage (the capacity tier). This enables you to reclaim

space on your primary storage and shrink secondary storage.

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

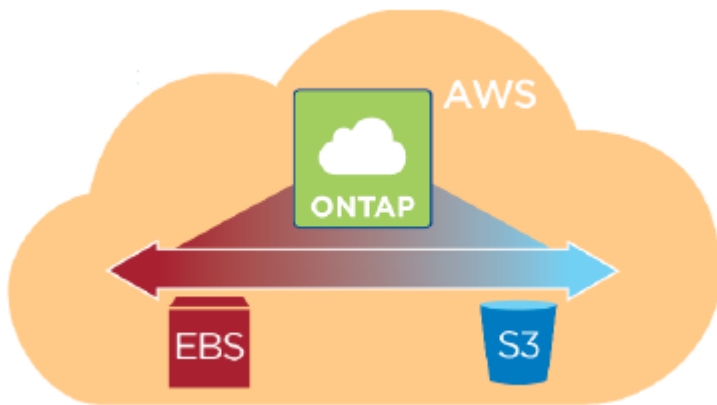


You do not need to install a feature license to enable data tiering.

- [How data tiering works in AWS](#)
- [How data tiering works in Microsoft Azure](#)
- [How data tiering affects capacity limits](#)
- [Volume tiering policies](#)
- [Setting up data tiering](#)

How data tiering works 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 cold data:



Performance tier in AWS

The performance tier can be General Purpose SSDs, Provisioned IOPS SSDs, or Throughput Optimized HDDs.

Capacity tier in AWS

By default, Cloud Volumes ONTAP tiers cold data to the S3 *Standard* storage class. Standard is ideal for frequently accessed data stored across multiple Availability Zones.

If you do not plan to access the cold data, you can reduce your storage costs by changing a system's tiering level to either of the following, after you deploy Cloud Volumes ONTAP:

Standard-Infrequent Access

For infrequently accessed data stored across multiple Availability Zones.

One Zone-Infrequent Access

For infrequently accessed data stored in a single Availability Zone.

The access costs are higher if you do access the data, so you must take that into consideration

before you change the tiering level. For more details about S3 storage classes, refer to [AWS documentation](#).

When you change the tiering level, cold data starts in the Standard storage class and moves to the storage class that you selected, if the data is not accessed after 30 days. For details about changing the tiering level, see [Tiering cold data to low-cost object storage](#).

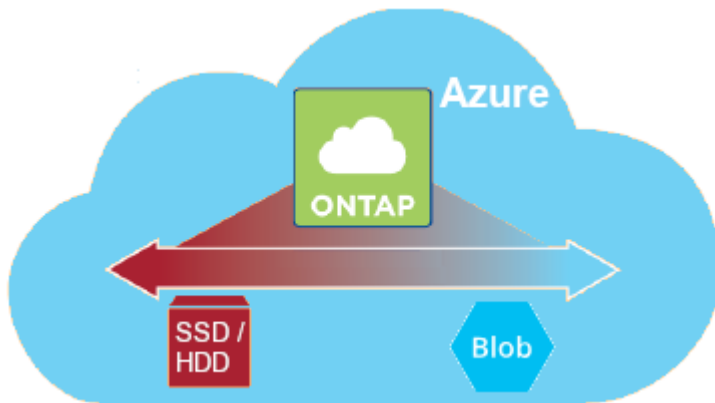
The tiering level is system wide—it is not per volume.



A Cloud Volumes ONTAP working environment uses an S3 bucket for all tiered data from the system. A different S3 bucket is not used for each volume. This includes an HA working environment. Cloud Manager creates an S3 bucket and names it *fabric-pool-cluster unique identifier*.

How data tiering works in Microsoft 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 cold data:



Performance tier in Azure

The performance tier can be either Premium Storage (SSD) or Standard Storage (HDD).

Capacity tier in Azure

By default, Cloud Volumes ONTAP tiers cold data to the Azure *hot* storage tier, which is ideal for frequently accessed data.

If you do not plan to access the cold data, you can reduce your storage costs by changing a system's tiering level to the Azure *cool* storage tier after you deploy Cloud Volumes ONTAP. The cool tier is ideal for infrequently accessed data that will reside in the tier for at least 30 days.

The access costs are higher if you do access the data, so you must take that into consideration before you change the tiering level. For more details about Azure Blob storage tiers, refer to [Azure documentation](#).

When you change the tiering level, cold data starts in the hot storage tier and moves to the cool storage tier, if the data is not accessed after 30 days. For details about changing the tiering level, see [Tiering cold data to low-cost object storage](#).

The tiering level is system wide—it is not per volume.



A Cloud Volumes ONTAP working environment uses an Azure Blob container for all tiered data from the system. A different container is not used for each volume. Cloud Manager creates a new storage account with a container for each Cloud Volumes ONTAP system. The name of the storage account is random.

How data tiering affects 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.

Cloud Volumes ONTAP supports the following tiering policies:

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.

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.

Backup

When you replicate a volume for disaster recovery or long-term retention, data for the destination volume starts in the capacity tier. If you activate the destination volume, the data gradually moves to the performance tier as it is read.

None

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

Setting up data tiering

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

1.4. 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.

1.4.1. 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 Cloud Manager 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.

1.4.2. Capacity management

The Cloud Manager 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

If the Cloud Manager Admin set the Capacity Management Mode to automatic, Cloud Manager automatically purchases new disks for Cloud Volumes ONTAP instances when more capacity is needed, deletes unused collections of disks (aggregates), and moves volumes between aggregates, as needed.

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.

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

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

Manual capacity management

If the Cloud Manager 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.

1.4.3. Storage isolation using tenants

Cloud Manager enables you to provision and manage storage in isolated groups called tenants. You need to decide how to organize Cloud Manager users and their working environments across tenants.

Working environments

Cloud Manager represents storage systems as *working environments*. A working environment is any of the following:

- A single Cloud Volumes ONTAP system or an HA pair
- An on-premises ONTAP cluster in your network
- An ONTAP cluster in a NetApp Private Storage configuration

The following image shows a Cloud Volumes ONTAP working environment:

[Screen shot: a Cloud Volumes ONTAP working environment, which shows Cloud Volumes ONTAP storage.]

Tenants

A *tenant* isolates working environments in groups. You create one or more working environments within a tenant. The following image shows three tenants defined in Cloud Manager:

[Screen shot: the Tenants page, which shows three defined tenants.]

User management of tenants and working environments

The tenants and working environments that Cloud Manager users can manage depend on user role and assignments. The three distinct user roles are as follows:

Cloud Manager Admin

Administers the product and can access all tenants and working environments.

Tenant Admin

Administers a single tenant. Can create and manage all working environments and users in the tenant.

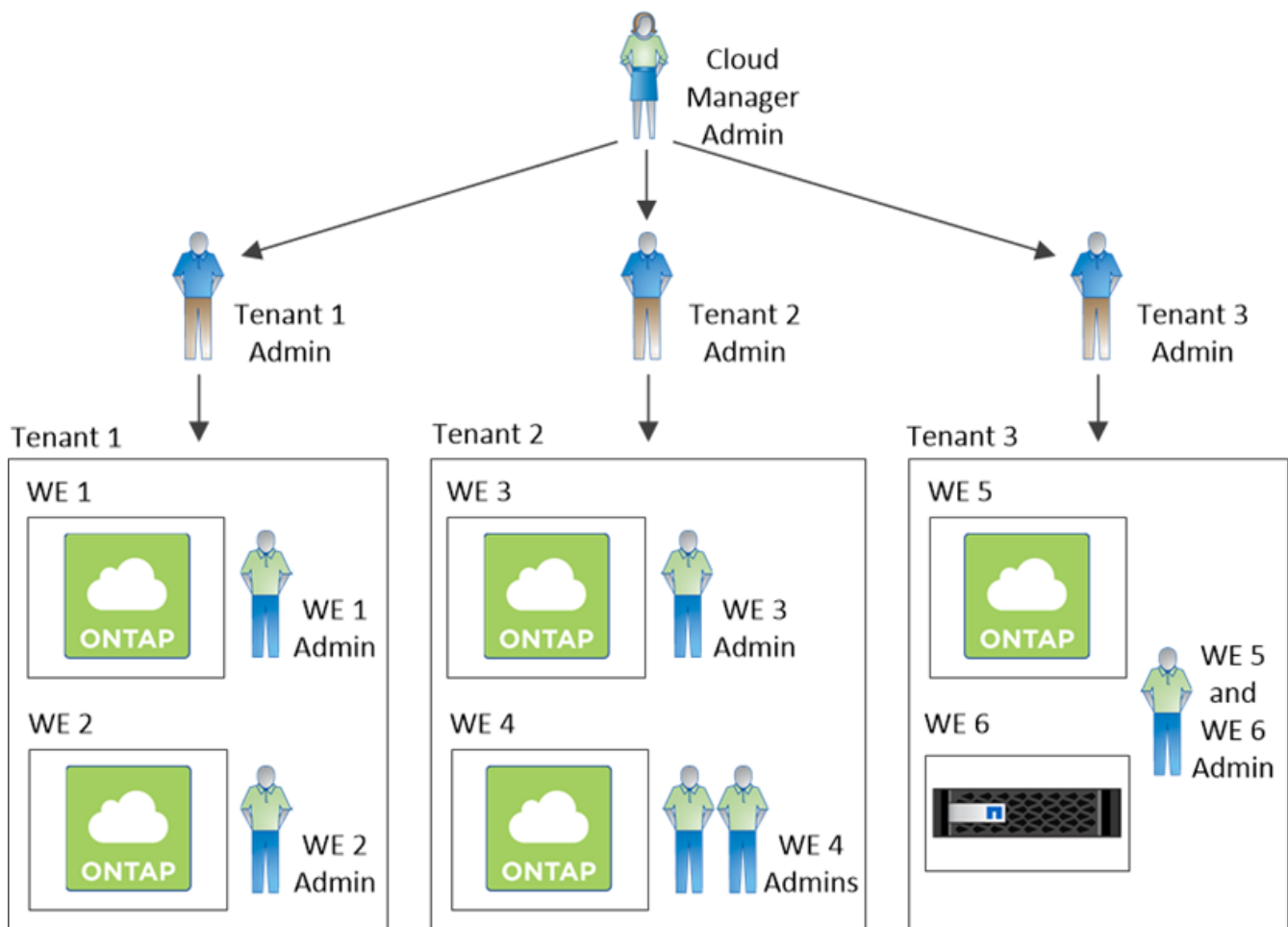
Working Environment Admin

Can create and manage one or more working environments in a tenant.

Example of how you can create tenants and users

If your organization has departments that operate independently, it is best to have a tenant for each department.

For example, you might create three tenants for three separate departments. You would then create a Tenant Admin for each tenant. Within each tenant would be one or more Working Environment Admins who manage working environments. The following image depicts this scenario:



Why you should link a tenant to your NetApp Support Site account

Cloud Manager prompts you to enter NetApp Support Site credentials for a tenant because it uses the credentials to manage licenses for Cloud Volumes ONTAP BYOL systems, to register pay-as-you-go instances for support, and to upgrade Cloud Volumes ONTAP software.

Watch the following video for more information about providing Cloud Manager with your NetApp Support Site credentials.

https://img.youtube.com/vi/_8s16fS_L1Y/maxresdefault.jpg

For step-by-step instructions and requirements for NetApp Support Site accounts, refer to [Linking tenants to a NetApp Support Site account](#).

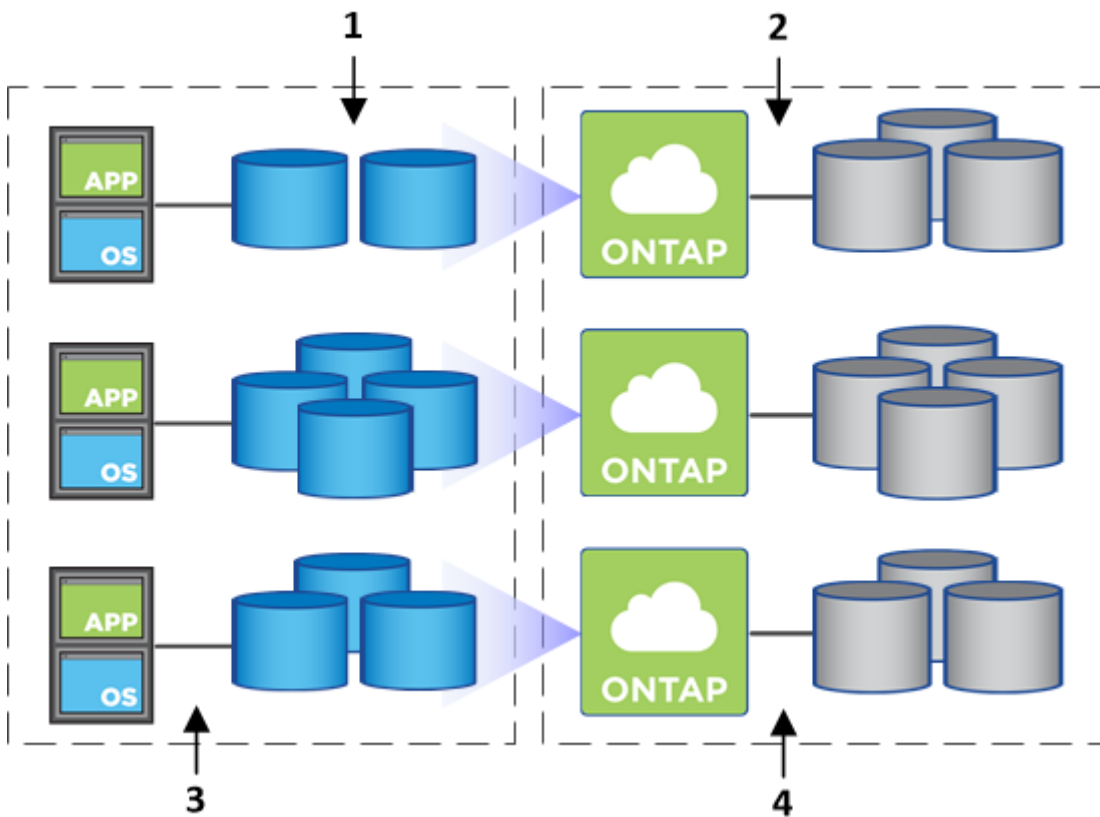
For more information about how Cloud Manager manages license files, refer to [Licensing](#).

1.4.4. Simplified storage management using the Volume View

Cloud Manager provides a separate management view called the *Volume View*, which further simplifies storage management in AWS.

The Volume View enables you to simply specify the NFS volumes that you need in AWS and then Cloud Manager handles the rest: it deploys Cloud Volumes ONTAP systems as needed and it makes capacity allocation decisions as volumes grow. This view gives you the benefits of enterprise-class storage in the cloud with very little storage management.

The following image shows how you interact with Cloud Manager in the Volume View:

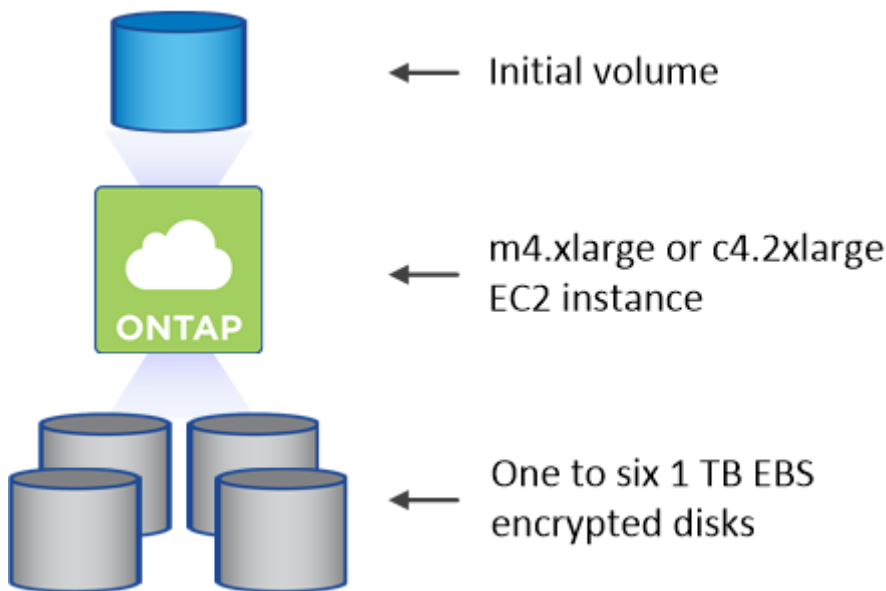


1. You create NFS volumes.
2. Cloud Manager launches Cloud Volumes ONTAP instances in AWS for new volumes or it creates volumes on existing instances. It also purchases physical EBS storage for the volumes.
3. You make the volumes available to your hosts and applications.
4. Cloud Manager makes capacity allocation decisions as your volumes grow.

This means that you simply need to interact with volumes (the image on the left), while Cloud Manager interacts with the storage system and its underlying storage (the image on the right).

Allocation of cloud resources for the initial volume

When you create your first volume, Cloud Manager launches a Cloud Volumes ONTAP instance or a Cloud Volumes ONTAP HA pair in AWS and purchases Amazon EBS storage for the volume:



The size of the initial volume determines the EC2 instance type and the number of EBS disks.



Cloud Manager launches a Cloud Volumes ONTAP Explore or Standard instance, depending on the initial volume size. As the volumes grow, Cloud Manager might prompt you to make an AWS instance change which means it needs to upgrade the instance's license to Standard or Premium. Upgrading increases the EBS raw capacity limit, which allows your volumes to grow.



Cloud Manager does not launch Cloud Volumes ONTAP BYOL instances in the Volume View. You should use Cloud Manager in the Storage System View if you purchased a Cloud Volumes ONTAP license.

Allocation of cloud resources for additional volumes

When you create additional volumes, Cloud Manager creates the volumes on existing Cloud Volumes ONTAP instances or on new Cloud Volumes ONTAP instances. Cloud Manager can create a volume on an existing instance if the instance's AWS location and disk type match the requested volume, and if there is enough space.

NetApp storage efficiency features and storage costs

Cloud Manager automatically enables NetApp storage efficiency features on all volumes. These efficiencies can reduce the total amount of storage that you need. You might see a difference between your allocated capacity and the purchased AWS capacity, which can result in storage cost savings.

Capacity allocation decisions that Cloud Manager automatically handles

- Cloud Manager purchases additional EBS disks as capacity thresholds are exceeded. This happens as your volumes grow.
- Cloud Manager deletes unused sets of EBS disks if the disks contain no volumes for 12 hours.
- Cloud Manager moves volumes between sets of disks to avoid capacity issues.

In some cases, this requires purchasing additional EBS disks. It also frees space on the original set of disks for new and existing volumes.

1.5. High-availability pairs

A Cloud Volumes ONTAP high availability (HA) configuration provides nondisruptive operations and fault tolerance. HA pairs are supported in AWS only.

1.5.1. Overview

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.

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.

1.5.2. Cloud Volumes ONTAP HA in 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 for clients within the VPC

When an HA configuration is spread across multiple Availability Zones, three floating IP addresses are required for NAS data access from within the VPC. 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.

These floating IP addresses are not natively accessible to clients that are outside of the VPC.

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.

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

NFS and CIFS data access for clients outside the VPC

When deployed in multiple AZs, Cloud Volumes ONTAP HA includes a separate set of IP addresses for NAS clients that are outside of the VPC. These IP addresses are static—they cannot migrate between nodes.

iSCSI data access

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

Storage takeover and giveback for iSCSI

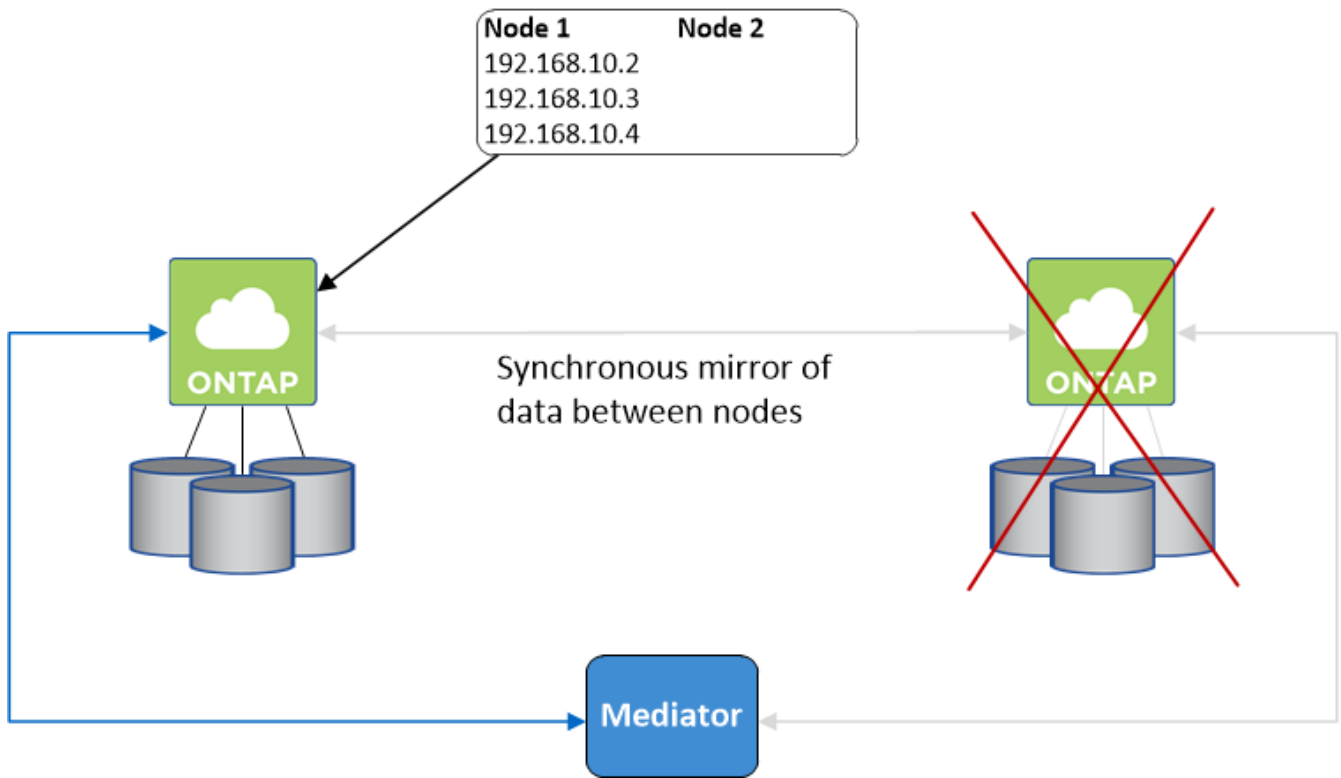
For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



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.

Storage 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**.

1.5.3. 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.

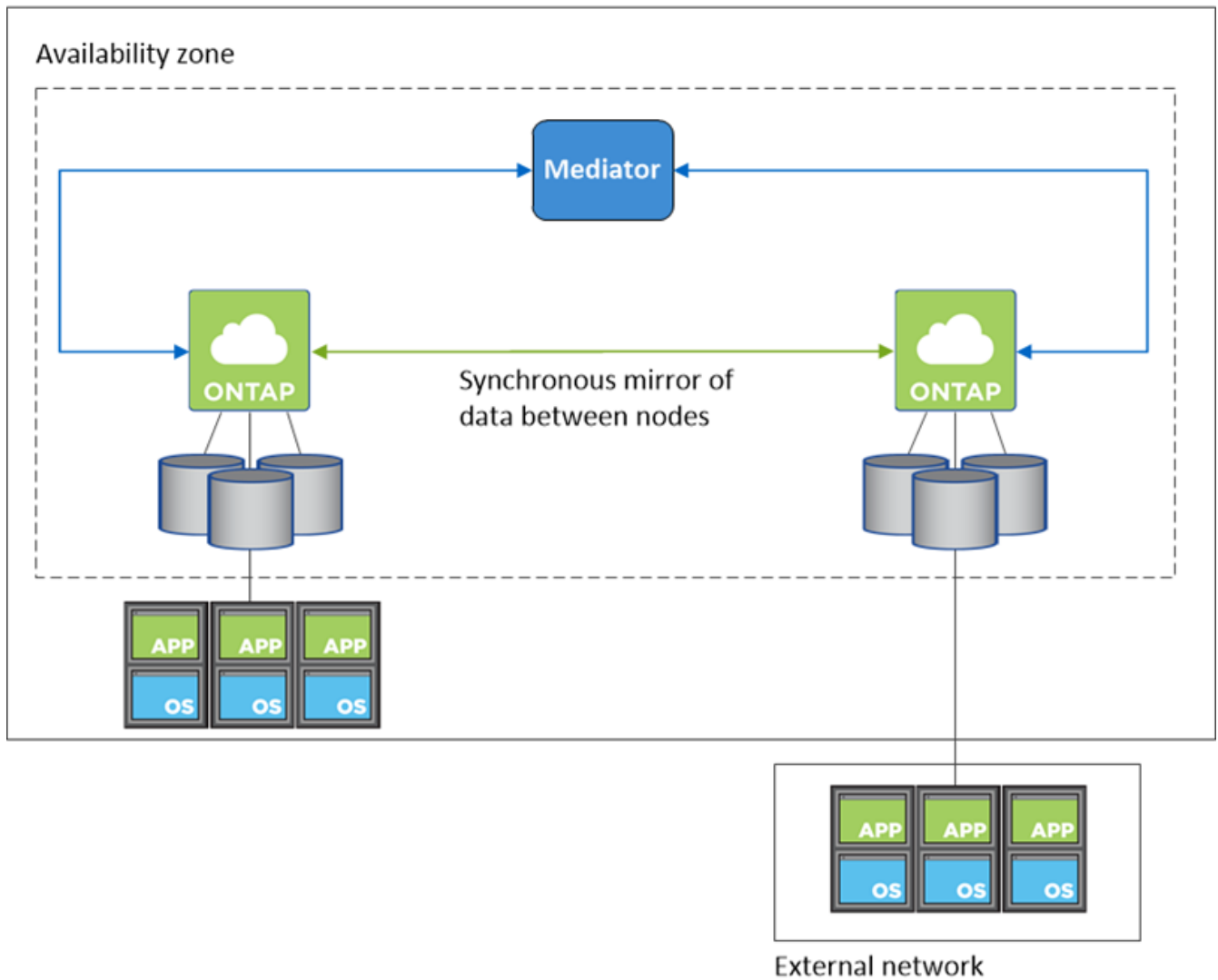


This HA configuration is not supported in the Volume View.

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.



Storage 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.

1.5.4. 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 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. The following image shows the Storage System View:

[Screen shot: Shows the Mount Command which is available when you select a volume.]

The following image shows the Volume View:

[Screen shot: Shows the menu options for a volume, which includes the Mount option.]

1.6. Security

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

1.6.1. Data encryption in Azure

[Azure Storage Service Encryption](#) for data at rest is enabled by default for Cloud Volumes ONTAP data in Azure.



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

1.6.2. Data encryption in AWS

Data encryption is supported in AWS using the [AWS Key Management Service \(KMS\)](#). Cloud Manager requests data keys using a customer master key (CMK).

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](#).

1.6.3. 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](#).

1.7. 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 cannot 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 specifying an activation code and setting the default retention period for files. You can obtain an activation code by using the chat icon in the lower right of the Cloud Manager interface.



You cannot 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:

[Shows the WORM option that is available when creating a new 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

- If you delete or move a disk directly from AWS or Azure, then a volume can be deleted before its expiry date.
- When WORM storage is activated, data tiering to object storage cannot be enabled.

1.8. Licensing

Each Cloud Volumes ONTAP BYOL system must have a license installed with an active subscription. If an active license is not installed, the Cloud Volumes ONTAP system shuts itself down after 30 days. Cloud Manager simplifies the process by managing licenses for you and by notifying you before they expire.

License management for a new system

A tenant must be linked to a NetApp Support Site account so Cloud Manager can obtain licenses for Cloud Volumes ONTAP BYOL systems. If the credentials are not present, Cloud Manager prompts you to enter them when you create a new Cloud Volumes ONTAP BYOL working environment.

For instructions, see [Linking tenants to a NetApp Support Site account](#).

Each time you launch a BYOL system, Cloud Manager automatically downloads the license from

NetApp and installs it on the Cloud Volumes ONTAP system.

If Cloud Manager cannot 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 warns you 30 days before a license is due to expire and again when the license expires. The following image shows a 30-day expiration warning:

[Screen shot: Shows a Cloud Volumes ONTAP working environment that includes a warning icon. The icon indicates that an action is required.]

You can select the working environment to review the message.

If you do not renew the license in time, the Cloud Volumes ONTAP system shuts itself down. If you restart it, it shuts itself down again.



Cloud Volumes ONTAP can also notify you through email, an SNMP traphost, or syslog server using EMS (Event Management System) event notifications. For instructions, see the [ONTAP 9 EMS Configuration Express Guide](#).

License renewal

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 cannot access the license file over the secure internet connection, you can obtain the file yourself and then manually upload the file to Cloud Manager. For instructions, see [Installing license files on Cloud Volumes ONTAP BYOL systems](#).

1.9. Performance

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

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

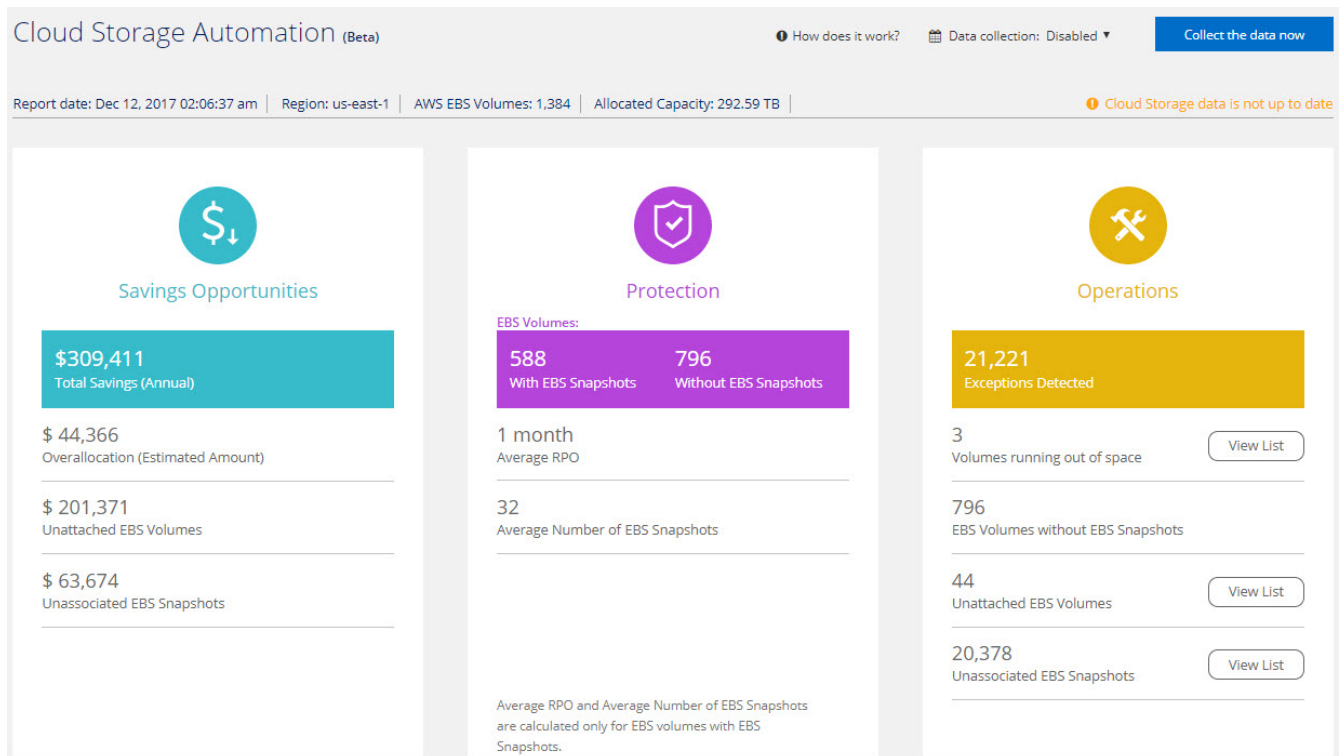
For Cloud Volumes ONTAP for Microsoft Azure, refer to [NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads](#).

1.10. Cloud Storage Automation

The Cloud Storage Automation Report analyzes your cloud storage to show you savings opportunities, data protection enhancements, and operations that can optimize the storage associated with your AWS account. This is a beta feature.

1.10.1. Sample report

The following image shows a sample report:



In some cases, the report enables you to take immediate action. For example, when you view the list of unattached EBS volumes or unassociated EBS snapshots, you can delete them right from Cloud Manager:

Unattached EBS Volumes

44 EBS Volumes 4 selected

<input type="checkbox"/>	EBS Volume ID	Type	Allocated Capacity	Tags	Creation Time	Deleting Status
<input checked="" type="checkbox"/>	vol-0f569b8cbb8f3728c	gp2	16 TB	None	Nov 20, 2017 07:30:27 pm	
<input checked="" type="checkbox"/>	vol-044641bbcfa5c0595	gp2	9.77 TB	None	Oct 27, 2017 09:16:26 am	
<input checked="" type="checkbox"/>	vol-0ba66d87777af9a39	gp2	9.77 TB	8 Tags ⓘ	Oct 28, 2017 04:12:54 pm	
<input checked="" type="checkbox"/>	vol-0d4b3a3a4b77e91a8	gp2	9.77 TB	None	Nov 6, 2017 06:34:48 pm	
<input type="checkbox"/>	vol-00acfb6e082030125	gp2	7.81 TB	None	Dec 1, 2017 02:36:25 am	
<input type="checkbox"/>	vol-0276f5ac55a477e67	gp2	7.81 TB	None	Oct 11, 2017 07:25:22 pm	
<input type="checkbox"/>	vol-0343fd60e5e62b29c	gp2	7.81 TB	None	Jul 21, 2017 07:32:42 pm	
<input type="checkbox"/>	vol-03f34df0e7c5c125e	gp2	7.81 TB	4 Tags ⓘ	Aug 24, 2017 04:22:02 pm	
<input type="checkbox"/>	vol-0476b62ea98a6743b	gp2	7.81 TB	None	Oct 10, 2017 05:54:46 pm	
<input type="checkbox"/>	vol-06d0f6c2164f21090	gp2	7.81 TB	None	Nov 16, 2017 06:56:51 pm	
<input type="checkbox"/>	vol-086e06fb6540c3386	gp2	7.81 TB	None	Oct 11, 2017 07:28:24 pm	

1.10.2. What happens when you enable the report

Cloud Manager collects information about the EC2 instances, EBS volumes, and EBS snapshots associated with your AWS account, in the region where Cloud Manager resides. AWS resources used for Cloud Volumes ONTAP are excluded. There is no performance impact on AWS resources.

When Cloud Manager collects the information, it identifies improvement opportunities by using EBS snapshots to calculate used capacity and daily usage growth predictions.

The report runs once a week, but you can initiate an immediate data collection at any time.

1.10.3. Required permissions

The AWS permissions required for Cloud Storage Automation are included in the Cloud Manager IAM policy. If you set up permissions correctly, then there is nothing further to do. See [Granting AWS permissions](#) for details.