NetApp

Cloud Volumes ONTAP documentation

Cloud Volumes ONTAP

NetApp
August 15, 2022

Table of Contents

Cloud Volumes ONTAP documentation

Release notes

What's new

Learn what's new with Cloud Volumes ONTAP management in Cloud Manager.

The enhancements described on this page are specific to Cloud Manager features that enable management of Cloud Volumes ONTAP. To learn what's new with the Cloud Volumes ONTAP software itself, go to the Cloud Volumes ONTAP Release Notes

31 July 2022

The following changes were introduced with the 3.9.21 release of the Connector.

MTEKM license

The Multi-tenant Encryption Key Management (MTEKM) license is now included with new and existing Cloud Volumes ONTAP systems running version 9.11.1 or later.

Multi-tenant external key management enables individual storage VMs (SVMs) to maintain their own keys through a KMIP server when using NetApp Volume Encryption.

Learn how to encrypt volumes with NetApp encryption solutions.

Proxy server

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

AutoSupport proactively monitors the health of your system and sends messages to NetApp technical support.

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

Change charging method

You can now change the charging method for a Cloud Volumes ONTAP system that uses capacity-based licensing. For example, if you deployed a Cloud Volumes ONTAP system with the Essentials package, you can change it to the Professional package if your business needs changed. This feature is available from the Digital Wallet.

Learn how to change charging methods.

Security group enhancement

When you create a Cloud Volumes ONTAP working environment, the user interface now enables you to choose whether you want the predefined security group to allow traffic within the selected network only (recommended) or all networks.
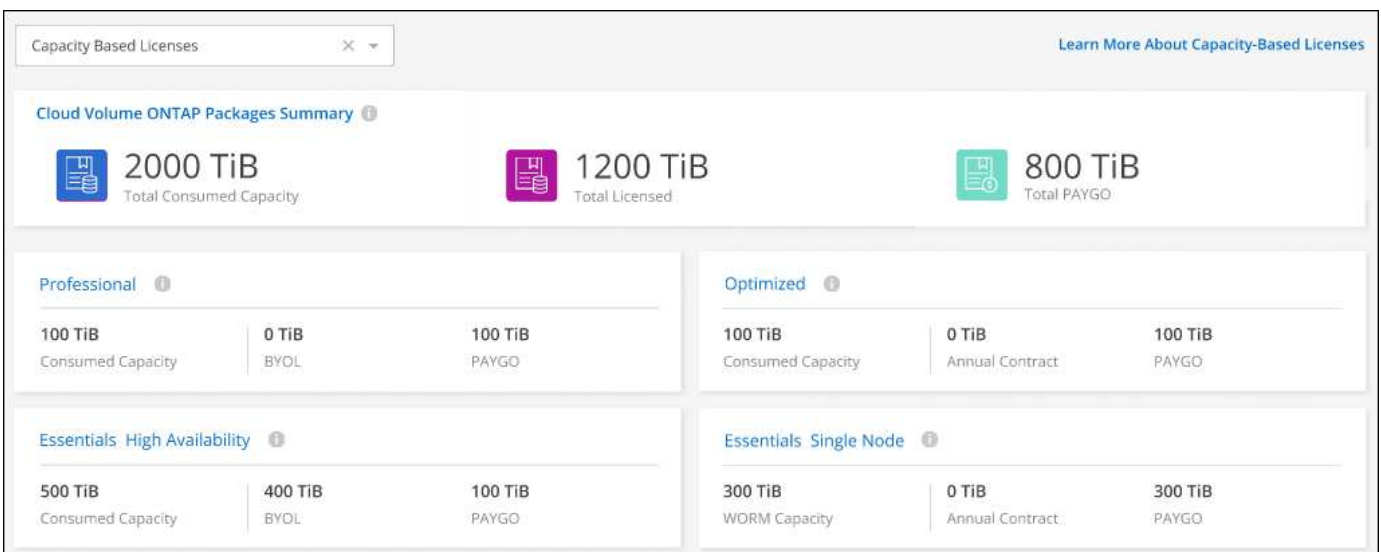
3 July 2022

The following changes were introduced with the 3.9.20 release of the Connector.

Digital Wallet

The Digital Wallet now shows you the total consumed capacity in your account and the consumed capacity by licensing package. This can help you understand how you're being charged and whether you need to purchase additional capacity.

Elastic Volumes enhancement

Cloud Manager now supports the Amazon EBS Elastic Volumes feature when creating a Cloud Volumes ONTAP working environment from the user interface. The Elastic Volumes feature is enabled by default when using gp3 or io1 disks. You can choose the initial capacity based on your storage needs and revise it after Cloud Volumes ONTAP is deployed.

Learn more about support for Elastic Volumes in AWS.

ONTAP S3 license in AWS

An ONTAP S3 license is now included on new and existing Cloud Volumes ONTAP systems running version 9.11.0 or later in AWS.

Learn how to configure and manage S3 object storage services in ONTAP

7 June 2022

The following changes were introduced with the 3.9.19 release of the Connector.

Cloud Volumes ONTAP 9.11.1

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.11.1, which includes support for new features and additional cloud provider regions.

Learn about the new features included in this release of Cloud Volumes ONTAP

New Advanced View

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using ONTAP System Manager, which is a management interface that's provided with an ONTAP system. We have included the System Manager interface directly inside Cloud Manager so that you don't need to leave Cloud Manager for advanced management.

This Advanced View is available as a Preview with Cloud Volumes ONTAP 9.10.0 and later. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Learn more about the Advanced View.

Support for Amazon EBS Elastic Volumes

Support for the Amazon EBS Elastic Volumes feature with a Cloud Volumes ONTAP aggregate provides better performance and additional capacity, while enabling Cloud Manager to automatically increase the underlying disk capacity as needed.

Support for Elastic Volumes is available starting with *new* Cloud Volumes ONTAP 9.11.0 systems and with gp3 and io1 EBS disk types.

Learn more about support for Elastic Volumes.

Note that support for Elastic Volumes requires new AWS permissions for the Connector:

```
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
```

Be sure to provide these permissions to each set of AWS credentials that you've added to Cloud Manager. View the latest Connector policy for AWS.

Support for deploying HA pairs in shared AWS subnets

Cloud Volumes ONTAP 9.11.1 includes support for AWS VPC sharing. This release of the Connector enables you to deploy an HA pair in an AWS shared subnet when using the API.

Learn how to deploy an HA pair in a shared subnet.

2 May 2022

The following changes were introduced with the 3.9.18 release of the Connector.

Cloud Volumes ONTAP 9.11.0

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.11.0.

Learn about the new features included in this release of Cloud Volumes ONTAP.

Enhancement to mediator upgrades

When Cloud Manager upgrades the mediator for an HA pair, it now validates that a new mediator image is available before it deletes the boot disk. This change ensures that the mediator can continue to operate successfully if the upgrade process is unsuccessful.

K8s tab has been removed

The K8s tab was deprecated in a previous and has now been removed. If you want to use Kubernetes with Cloud Volumes ONTAP, you can add managed-Kubernetes clusters to the Canvas as a working environment for advanced data management.

Learn about Kubernetes data management in Cloud Manager

S3 Glacier Instant Retrieval

You can now store tiered data in the Amazon S3 Glacier Instant Retrieval storage class.

Learn how to change the storage class for tiered data.

New AWS permissions required for the Connector

The following permissions are now required to create an AWS spread placement group when deploying an HA pair in a single Availability Zone (AZ):

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

These permissions are now required to optimize how Cloud Manager creates the placement group.

Be sure to provide these permissions to each set of AWS credentials that you've added to Cloud Manager. View the latest Connector policy for AWS.

3 April 2022

System Manager link has been removed

We have removed the System Manager link that was previously available from within a Cloud Volumes ONTAP working environment.

You can still connect to System Manager by entering the cluster management IP address in a web browser that has a connection to the Cloud Volumes ONTAP system. Learn more about connecting to System Manager.

Charging for WORM storage

Now that the introductory special rate has expired, you will now be charged for using WORM storage. Charging is hourly, according to the total provisioned capacity of WORM volumes. This applies to new and existing Cloud Volumes ONTAP systems.

Learn about pricing for WORM storage.

27 February 2022

The following changes were introduced with the 3.9.16 release of the Connector.

Redesigned volume wizard

The create new volume wizard that we recently introduced is now available when creating a volume on a specific aggregate from the **Advanced allocation** option.

Learn how to create volumes on a specific aggregate.

9 February 2022

Marketplace updates

- The Essentials package and Professional package are now available in all cloud provider marketplaces.

  These by-capacity charging methods enable you to pay by the hour or to purchase an annual contract directly from your cloud provider. You still have the option to purchase a by-capacity license directly from NetApp.

  If you have an existing subscription in a cloud marketplace, you're automatically subscribed to these new offerings as well. You can choose by-capacity charging when you deploy a new Cloud Volumes ONTAP working environment.

  If you're a new customer, Cloud Manager will prompt you to subscribe when you create a new working environment.

- By-node licensing from all cloud provider marketplaces is deprecated and no longer available for new subscribers. This includes annual contracts and hourly subscriptions (Explore, Standard, and Premium).

This charging method is still available for existing customers who have an active subscription.

Learn more about the licensing options for Cloud Volumes ONTAP.

6 February 2022

Exchange unassigned licenses

If you have an unassigned node-based license for Cloud Volumes ONTAP that you haven't used, you can now exchange the license by converting it to a Cloud Backup license, Cloud Data Sense license, or Cloud Tiering license.

This action revokes the Cloud Volumes ONTAP license and creates a dollar-equivalent license for the service with the same expiry date.

Learn how to exchange unassigned node-based licenses.

30 January 2022

The following changes were introduced with the 3.9.15 release of the Connector.

Redesigned licensing selection

We redesigned the licensing selection screen when creating a new Cloud Volumes ONTAP working environment. The changes highlight the by-capacity charging methods that were introduced in July 2021 and support upcoming offerings through the cloud provider marketplaces.

Digital Wallet update

We updated the **Digital Wallet** by consolidating Cloud Volumes ONTAP licenses in a single tab.

2 January 2022

The following changes were introduced with the 3.9.14 release of the Connector.

FlexClone charging update

If you use a capacity-based license for Cloud Volumes ONTAP, you are no longer charged for the capacity used by FlexClone volumes.

Charging method now displayed

Cloud Manager now shows the charging method for each Cloud Volumes ONTAP working environment in the right panel of the Canvas.

Choose your user name

When you create a Cloud Volumes ONTAP working environment, you now have the option to enter your preferred user name, instead of the default admin user name.

Volume creation enhancements

We made a few enhancements to volume creation:

- We redesigned the create volume wizard for ease of use.
- Tags that you add to a volume are now associated with the Application Templates service, which can help you organize and simplify the management of your resources.

- You can now choose a custom export policy for NFS.

28 November 2021

The following changes were introduced with the 3.9.13 release of the Connector.

Cloud Volumes ONTAP 9.10.1

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.10.1.

Learn about the new features included in this release of Cloud Volumes ONTAP.

Keystone Flex Subscriptions

You can now use Keystone Flex Subscriptions to pay for Cloud Volumes ONTAP HA pairs.

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service that delivers a seamless hybrid cloud experience for those preferring OpEx consumption models to upfront CapEx or leasing.

A Keystone Flex Subscription is supported with all new versions of Cloud Volumes ONTAP that you can deploy from Cloud Manager.

- Learn more about Keystone Flex Subscriptions.
- Learn how to get started with Keystone Flex Subscriptions in Cloud Manager.

New AWS region support

Cloud Volumes ONTAP is now supported in the AWS Asia Pacific (Osaka) region (ap-northeast-3).

4 October 2021

The following changes were introduced with the 3.9.11 release of the Connector.

Cloud Volumes ONTAP 9.10.0

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.10.0.

7 July 2021

The following changes were introduced with the 3.9.8 release of the Connector.

New charging methods

New charging methods are available for Cloud Volumes ONTAP.

- **Capacity-based BYOL**: A capacity-based license enables you to pay for Cloud Volumes ONTAP per TiB of capacity. The license is associated with your NetApp account and enables you to create as multiple Cloud Volumes ONTAP systems, as long as enough capacity is available through your license. Capacity-based licensing is available in the form of a package, either *Essentials* or *Professional*.

- **Freemium offering**: Freemium 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 system and there's no support contract. You can have up to 10 Freemium systems.

  Learn more about these licensing options.

  Here's an example of the charging methods that you can choose from:

WORM storage available for general use

Write once, read many (WORM) storage is no longer in Preview and is now available for general use with Cloud Volumes ONTAP. Learn more about WORM storage.

Support for m5dn.24xlarge in AWS

Starting with the 9.9.1 release, Cloud Volumes ONTAP now supports the m5dn.24xlarge instance type with the following charging methods: PAYGO Premium, bring your own license (BYOL), and Freemium.

View supported configurations for Cloud Volumes ONTAP in AWS.

30 May 2021

The following changes were introduced with the 3.9.7 release of the Connector.

New Professional Package in AWS

A new Professional Package enables you to bundle Cloud Volumes ONTAP and Cloud Backup Service by using an annual contract from the AWS Marketplace. Payment is per TiB. This subscription doesn't enable you to back up on-prem data.

If you choose this payment option, you can provision up to 2 PiB per Cloud Volumes ONTAP system through EBS disks and tiering to S3 object storage (single node or HA).

Go to the AWS Marketplace page to view pricing details and go to the Cloud Volumes ONTAP Release Notes to learn more about this licensing option.

Tags on EBS volumes in AWS

Cloud Manager now adds tags to EBS volumes when it creates a new Cloud Volumes ONTAP working environment. The tags were previously created after Cloud Volumes ONTAP was deployed.

This change can help if your organization uses service control policies (SCPs) to manage permissions.

Minimum cooling period for auto tiering policy

If you enabled data tiering on a volume using the *auto* tiering policy, you can now adjust the minimum cooling period using the API.

Learn how to adjust the minimum cooling period.

Enhancement to custom export policies

When you create a new NFS volume, Cloud Manager now displays custom export policies in ascending order, making it easier for you to find the export policy that you need.

Deletion of old cloud snapshots

Cloud Manager now deletes older cloud snapshots of root and boot disks that are created when a Cloud Volumes ONTAP system is deployed and every time its powered down. Only the two most recent snapshots are retained for both the root and boot volumes.

This enhancement helps reduce cloud provider costs by removing snapshots that are no longer needed.

24 May 2021

Cloud Volumes ONTAP 9.9.1

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.9.1.

Learn about the new features included in this release of Cloud Volumes ONTAP.

11 Apr 2021

The following changes were introduced with the 3.9.5 release of the Connector.

Logical space reporting

Cloud Manager now enables logical space reporting on the initial storage VM that it creates for Cloud Volumes ONTAP.

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.

Support for gp3 disks in AWS

Cloud Volumes ONTAP now supports *General Purpose SSD (gp3)* disks, starting with the 9.7 release. gp3 disks are the lowest-cost SSDs that balance cost and performance for a broad range of workloads.

Learn more about using gp3 disks with Cloud Volumes ONTAP.

Cold HDD disks no longer supported in AWS

Cloud Volumes ONTAP no longer supports Cold HDD (sc1) disks.

8 Mar 2021

The following changes were introduced with the 3.9.4 release of the Connector.

Cloud Volumes ONTAP 9.9.0

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.9.0.

Learn about the new features included in this release of Cloud Volumes ONTAP.

Support for the AWS C2S environment

You can now deploy Cloud Volumes ONTAP 9.8 in the AWS Commercial Cloud Services (C2S) environment.

Learn how to get started in C2S.

AWS encryption with customer-managed CMKs

Cloud Manager has always enabled you to encrypt Cloud Volumes ONTAP data using the AWS Key Management Service (KMS). Starting with Cloud Volumes ONTAP 9.9.0, data on EBS disks and data tiered to S3 are encrypted if you select a customer-managed CMK. Previously, only EBS data would be encrypted.

Note that you'll need to provide the Cloud Volumes ONTAP IAM role with access to use the CMK.

Learn more about setting up the AWS KMS with Cloud Volumes ONTAP.

4 Jan 2021

The following changes were introduced with the 3.9.2 release of the Connector.

AWS Outposts

A few months ago, we announced that Cloud Volumes ONTAP had achieved the Amazon Web Services (AWS) Outposts Ready designation. Today, we're pleased to announce that we've validated Cloud Manager and Cloud Volumes ONTAP with AWS Outposts.

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

There are a few limitations to point out:

- Only single node Cloud Volumes ONTAP systems are supported at this time
- The EC2 instances that you can use with Cloud Volumes ONTAP are limited to what's available in your Outpost
- Only General Purpose SSDs (gp2) are supported at this time

Known limitations

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

These limitations are specific to Cloud Volumes ONTAP management in Cloud Manager. To view limitations with the Cloud Volumes ONTAP software itself, go to the Cloud Volumes ONTAP Release Notes

Cloud Manager doesn't support FlexGroup volumes

While Cloud Volumes ONTAP supports FlexGroup volumes, Cloud Manager does not. If you create a FlexGroup volume from System Manager or from the CLI, then you should set Cloud Manager's Capacity Management mode to Manual. Automatic mode might not work properly with FlexGroup volumes.

Cloud Manager doesn't support S3 with Cloud Volumes ONTAP

While Cloud Volumes ONTAP supports S3 as an option for scale-out storage in some cloud providers, Cloud Manager doesn't provide any management capabilities for this feature. Using the CLI is the best practice to configure S3 client access from Cloud Volumes ONTAP. For details, refer to the S3 Configuration Power Guide.

Learn more about Cloud Volumes ONTAP support for S3 and other client protocols.

Cloud Manager doesn't support disaster recovery for storage VMs

Cloud Manager doesn't provide any setup or orchestration support for storage VM disaster recovery. You must use System Manager or the CLI.

- SVM Disaster Recovery Preparation Express Guide
- SVM Disaster Recovery Express Guide

Cloud Volumes ONTAP Release Notes

The Release Notes for Cloud Volumes ONTAP provide release-specific information. What's new in the release, supported configurations, storage limits, and any known limitations or issues that can affect product functionality.

Go to the Cloud Volumes ONTAP Release Notes

Get started

Learn about Cloud Volumes ONTAP

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

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

- Storage efficiencies

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

- High availability

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

- Data protection

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

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

  Learn more about Cloud Backup

- Data tiering

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

- Application consistency

  Ensure consistency of NetApp Snapshot copies using NetApp SnapCenter.

  Learn more about SnapCenter

- Data security

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

- Privacy compliance controls

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

  Learn more about Cloud Data Sense

> (i) Licenses for ONTAP features are included with Cloud Volumes ONTAP.

View supported Cloud Volumes ONTAP configurations

Get started in Amazon Web Services

Quick start for Cloud Volumes ONTAP in AWS

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

1 **Create a Connector**

If you don't have a Connector yet, an Account Admin needs to create one. Learn how to create a Connector in AWS.

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

2 **Plan your configuration**

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

3 **Set up your networking**

a. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.

b. Enable outbound internet access from the target VPC so the Connector and Cloud Volumes ONTAP can contact several endpoints.

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

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

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

Learn more about networking requirements.

4 **Set up the AWS KMS**

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

5 **Launch Cloud Volumes ONTAP using Cloud Manager**

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

Related links

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

Plan your Cloud Volumes ONTAP configuration in AWS

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

Choose a Cloud Volumes ONTAP license

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

- Learn about licensing options for Cloud Volumes ONTAP
- Learn how to set up licensing

Choose a supported region

Cloud Volumes ONTAP is supported in most AWS regions. View the full list of supported regions.

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

Choose a supported instance

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

Supported configurations for Cloud Volumes ONTAP in AWS

Understand storage limits

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

Storage limits for Cloud Volumes ONTAP in AWS

Size your system in AWS

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

Instance type

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

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

EBS disk type

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

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

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

  Note that Cloud Volumes ONTAP supports the Amazon EBS Elastic Volumes feature with gp3 disks. Learn more about Elastic Volumes support.

- *General Purpose SSD (gp2)* disks balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS.

- *Provisioned IOPS SSD (io1)* disks are for critical applications that require the highest performance at a higher cost.

  Note that Cloud Volumes ONTAP supports the Amazon EBS Elastic Volumes feature with io1 disks. Learn more about Elastic Volumes support.

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

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

EBS disk size

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

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

For more details about EBS disk performance, refer to AWS Documentation: EBS Volume Types.

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

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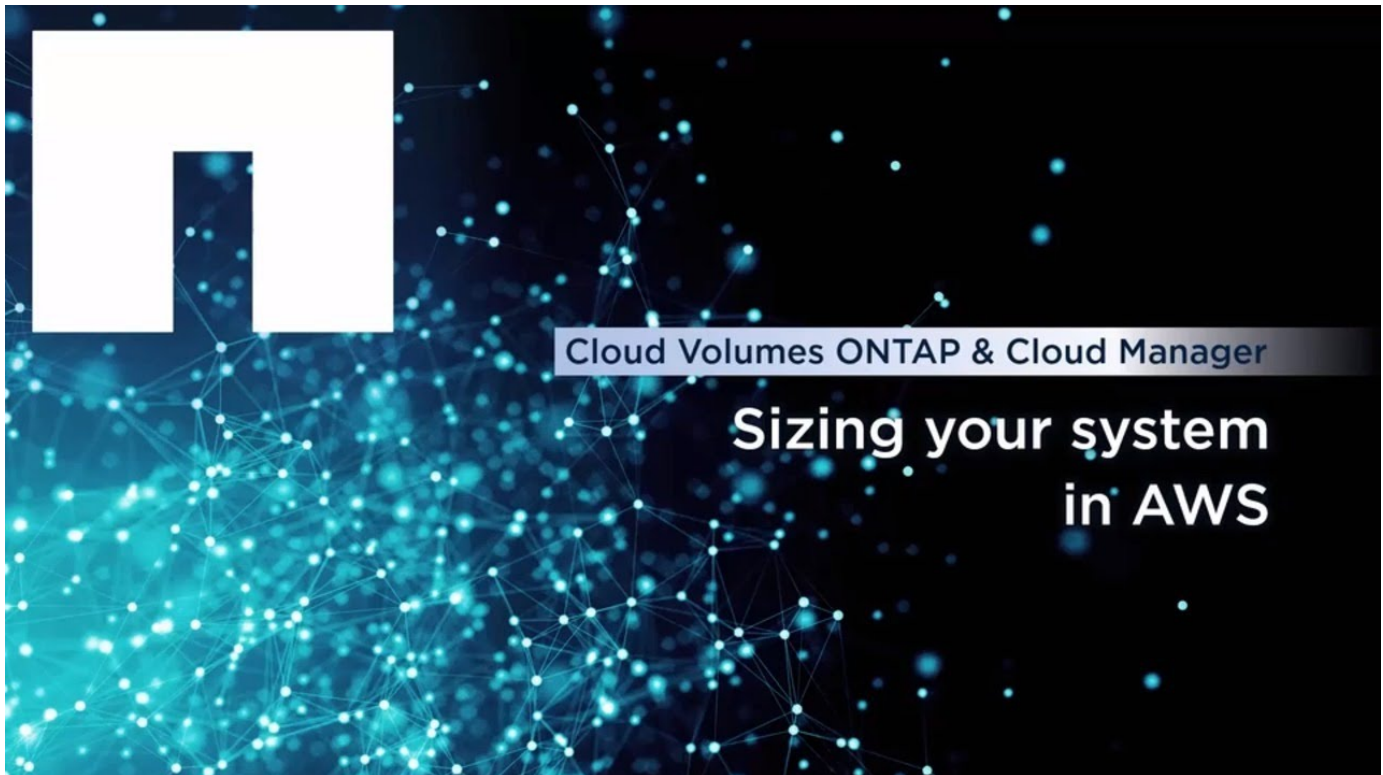
View default system disks

In addition to the storage for user data, Cloud Manager also purchases cloud storage for Cloud Volumes ONTAP system data (boot data, root data, core data, and NVRAM). For planning purposes, it might help for you to review these details before you deploy Cloud Volumes ONTAP.

View the default disks for Cloud Volumes ONTAP system data in AWS.

> The Connector also requires a system disk. View details about the Connector's default configuration.

Prepare to deploy Cloud Volumes ONTAP in an AWS Outpost

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

There are a few limitations to point out:

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

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

Collect networking information

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

Single node or HA pair in a single AZ

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

HA pair in multiple AZs

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

Choose a write speed

Cloud Manager enables you to choose a write speed setting for Cloud Volumes ONTAP. Before you choose a write speed, you should understand the differences between the normal and high settings and risks and

recommendations when using high write speed. [Learn more about write speed](#).

Choose a volume usage profile

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

NetApp storage efficiency features provide the following benefits:

Thin provisioning

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

Deduplication

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

Compression

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

Set up your networking

Networking requirements for Cloud Volumes ONTAP in AWS

Cloud Manager handles the set up of networking components for Cloud Volumes ONTAP, such as IP addresses, netmasks, and routes. You need to make sure that outbound internet access is available, that enough private IP addresses are available, that the right connections are in place, and more.

General requirements

The following requirements must be met in AWS.

Outbound internet access for Cloud Volumes ONTAP nodes

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

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

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

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

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

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

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

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

Outbound internet access for the HA mediator

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

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

Private IP addresses

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

The number of LIFs that Cloud Manager allocates for Cloud Volumes ONTAP depends on whether you deploy a single node system or an HA pair. A LIF is an IP address associated with a physical port.

IP addresses for a single node system

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

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

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

IP addresses for HA pairs

HA pairs require more IP addresses than a single node system does. These IP addresses are spread across different ethernet interfaces, as shown in the following image:
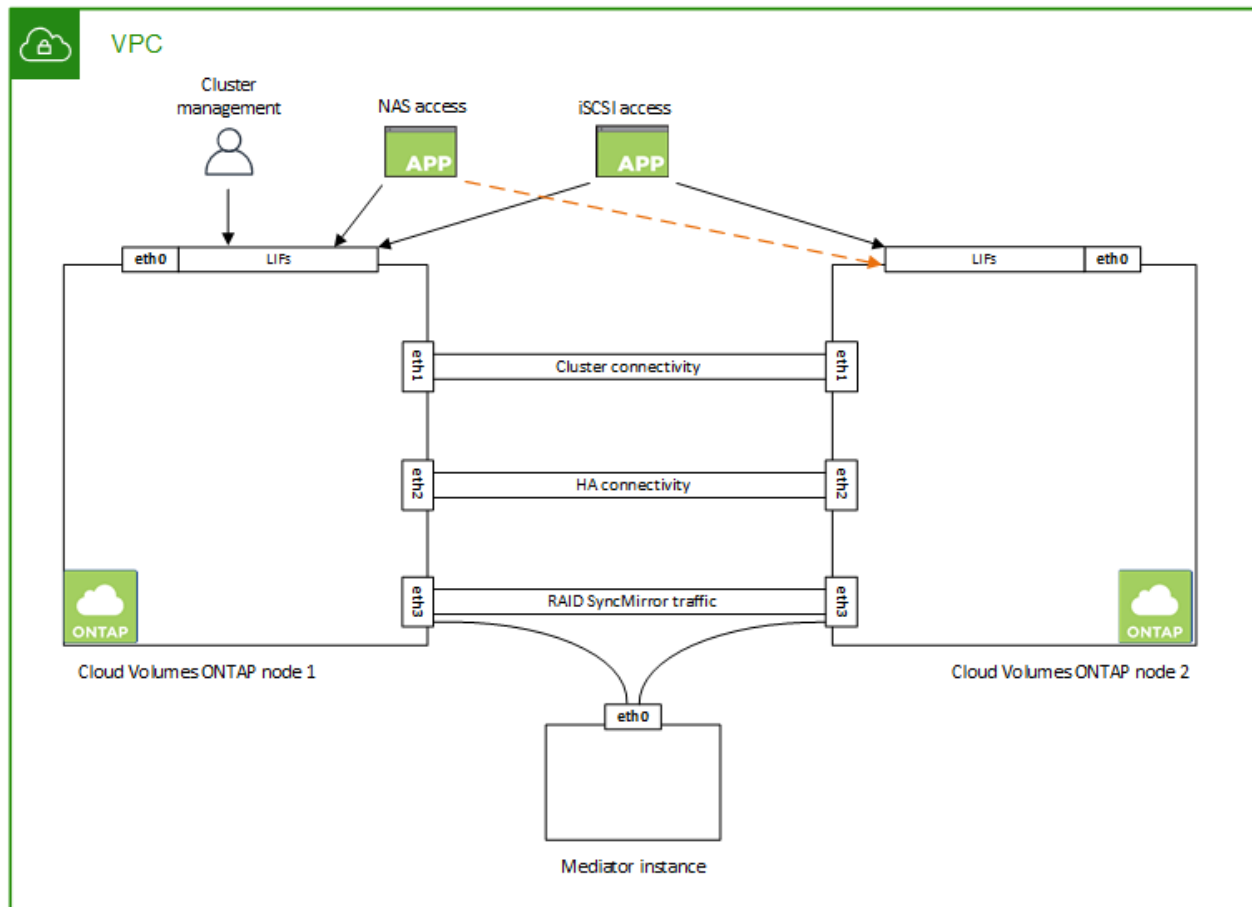
The number of private IP addresses required for an HA pair depends on which deployment model you choose. An HA pair deployed in a *single* AWS Availability Zone (AZ) requires 15 private IP addresses, while an HA pair deployed in *multiple* AZs requires 13 private IP addresses.

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

LIFs for HA pairs in a single AZ

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

LIF	Interface	Node	Purpose
Cluster connectivity	eth1	node 1 and node 2	Enables the nodes to communicate with each other and to move data within the cluster.
HA connectivity	eth2	node 1 and node 2	Communication between the two nodes in case of failover.
RSM iSCSI traffic	eth3	node 1 and node 2	RAID SyncMirror iSCSI traffic, as well as communication between the two Cloud Volumes ONTAP nodes and the mediator.
Mediator	eth0	Mediator	A communication channel between the nodes and the mediator to assist in storage takeover and giveback processes.

LIFs for HA pairs in multiple AZs

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

> 💡 When deployed in multiple Availability Zones, several LIFs are associated with floating IP addresses, which don't count against the AWS private IP limit.

Security groups

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

Connection for data tiering

If you want to use EBS as a performance tier and AWS S3 as a capacity tier, you must ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC

Endpoint to the S3 service. For instructions, see AWS Documentation: Creating a Gateway Endpoint.

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

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

Connections to ONTAP systems

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

DNS and Active Directory for CIFS

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

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

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

VPC sharing

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

Learn how to deploy an HA pair in a shared subnet.

Requirements for HA pairs in multiple AZs

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

To understand how HA pairs work, see High-availability pairs.

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

A subnet should be available in each Availability Zone.

Floating IP addresses for NAS data and cluster/SVM management
    HA configurations in multiple AZs use floating IP addresses that migrate between nodes if failures occur. They are not natively accessible from outside the VPC, unless you set up an AWS transit gateway.

    One floating IP address is for cluster management, one is for NFS/CIFS data on node 1, and one is for

NFS/CIFS data on node 2. A fourth floating IP address for SVM management is optional.

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

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

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

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

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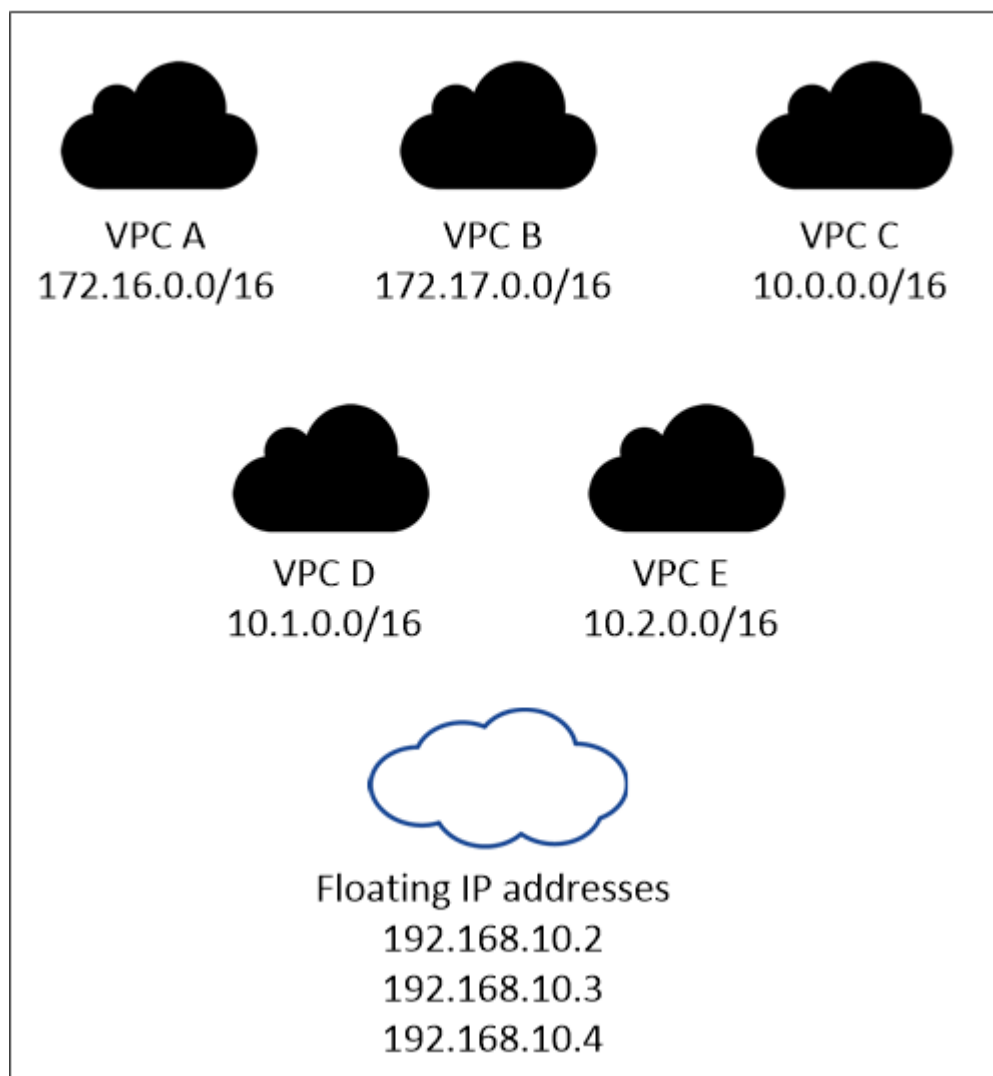
> (i) Cloud Manager automatically creates static IP addresses for iSCSI access and for NAS access from clients outside the VPC. You don't need to meet any requirements for these types of IP addresses.

Transit gateway to enable floating IP access from outside the VPC

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

Route tables

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

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

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

For more information about route tables, refer to AWS Documentation: Route Tables.

Connection to NetApp management tools

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

1. Deploy the NetApp management tools in a different VPC and set up an AWS transit gateway. The gateway enables access to the floating IP address for the cluster management interface from outside the VPC.

2. Deploy the NetApp management tools in the same VPC with a similar routing configuration as NAS clients.

Example HA configuration

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

Floating IP addresses in one or more route tables

Node 1	Node 2
192.168.10.2	192.168.10.4
192.168.10.3	

Virtual Private Cloud
172.31.0.0/16

Availability zone 1

Subnet 1

ONTAP

Synchronous mirror of data between nodes

Availability zone 2

Subnet 2

ONTAP

APP OS   APP OS   APP OS

Availability zone 3

Subnet 3

Mediator
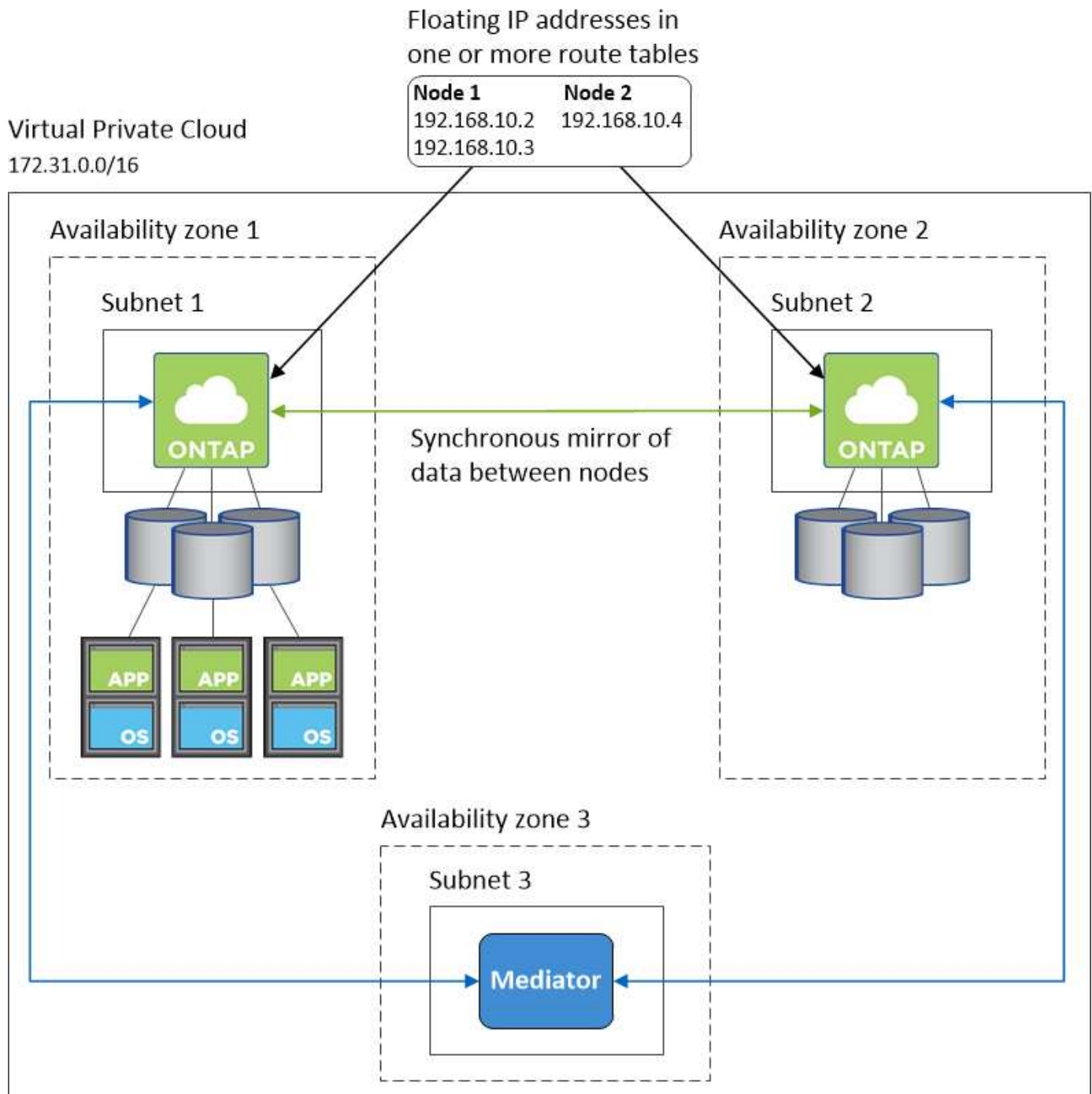
Requirements for the Connector

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

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

Connection to target networks

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

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

Outbound internet access

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

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

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

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

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

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

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

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

172.23.0.1
172.23.0.2
172.23.0.3
172.23.0.4

Floating IPs
routed to VPC1
route table

Transit
gateway

172.23.0.1
172.23.0.2
172.23.0.3
172.23.0.4

Floating IPs
routed to ENIs

Mediator

ONTAP

ONTAP

VPC 1 (10.160.0.0/20)

172.23.0.1
172.23.0.2
172.23.0.3
172.23.0.4

Floating IPs
routed to the
transit gateway

APP

OS

Client

VPC 2 (10.100.0.0/16)

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

Steps

1. Create a transit gateway and attach the VPCs to the gateway.

2. Associate the VPCs with the transit gateway route table.

   a. In the **VPC** service, click **Transit Gateway Route Tables**.

   b. Select the route table.

   c. Click **Associations** and then select **Create association**.

   d. Choose the attachments (the VPCs) to associate and then click **Create association**.

3. Create routes in the transit gateway's route table by specifying the HA pair's floating IP addresses.

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

NFS & CIFS access from within the VPC using Floating IP

ⓘ **Auto failover**

Cluster Management :	172.23.0.1
Data (nfs,cifs) :	Node 1: 172.23.0.2 | Node 2: 172.23.0.3

Access

SVM Management :	172.23.0.4

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

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

    a. Add route entries to the floating IP addresses.

    b. Add a route entry to the CIDR block of the VPC where the HA pair resides.

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

Route Table: rtb-0569a1bd740ed033f

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

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

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

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

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

6. Mount volumes to clients using the floating IP address.

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

Volumes

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

vol1 ⓘ Info   ✏ Edit   🗑 Delete   ✕

🗐 Clone   ⬀ Mount Command

↺ Restore from Snapshot copy   ⬛ Change Tier

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

   Learn how to edit a volume.

Related links

- High-availability pairs in AWS
- Networking requirements for Cloud Volumes ONTAP in AWS

Deploy an HA pair in a shared subnet

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

With VPC sharing, a Cloud Volumes ONTAP HA configuration is spread across two accounts:

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

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

The following image shows the components involved this deployment:

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

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

Steps

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

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

   AWS documentation: Share a subnet

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

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

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

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

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

   Note that you must specify the following fields:

   ◦ "securityGroupId"

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

   ◦ "assumeRoleArn" in the "haParams" object

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

   For example:

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

   Learn about the Cloud Volumes ONTAP API

Security group rules for AWS

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

Rules for Cloud Volumes ONTAP

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

Inbound rules

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

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

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the System Manager web console using the IP address of the cluster management LIF
HTTPS	443	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
UDP	635	NFS mount
UDP	2049	NFS server daemon
UDP	4045	NFS lock daemon

Protocol	Port	Purpose
UDP	4046	Network status monitor for NFS
UDP	4049	NFS rquotad protocol

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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

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

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

Service	Protocol	Port	Source	Destination	Purpose
AutoSupport	HTTPS	443	Node management LIF	support.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	support.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Connector	Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available
Backup to S3	TCP	5010	Intercluster LIF	Backup endpoint or restore endpoint	Back up and restore operations for the Backup to S3 feature
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
	TCP	3000	Node management LIF	HA mediator	ZAPI calls (Cloud Volumes ONTAP HA only)
	ICMP	1	Node management LIF	HA mediator	Keep alive (Cloud Volumes ONTAP HA only)
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Node management LIF	Destination servers	NDMP copy
SMTP	TCP	25	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	TCP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	TCP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
SnapMirror	TCP	11104	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	11105	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer

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

Rules for the HA mediator external security group

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

Inbound rules

The source for inbound rules is 0.0.0.0/0.

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

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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

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

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

Rules for the HA configuration internal security group

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

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

Inbound rules

The predefined security group includes the following inbound rules.

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

Outbound rules

The predefined security group includes the following outbound rules.

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

Rules for the Connector

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

Inbound rules

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

Outbound rules

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

Basic outbound rules

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

Protocol	Port	Purpose
All TCP	All	All outbound traffic

Protocol	Port	Purpose
All UDP	All	All outbound traffic

Advanced outbound rules

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

ⓘ The source IP address is the Connector host.

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

Setting up the AWS KMS

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

Steps

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

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

   AWS Documentation: Customer Master Keys (CMKs)

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

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

   AWS Documentation: Editing Keys

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

   a. Go to the KMS console from the account where the CMK resides.

   b. Select the key.

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

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

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

   In most cases, this is the account where Cloud Manager resides. If Cloud Manager wasn't installed in AWS, it would be the account for which you provided AWS access keys to Cloud Manager.
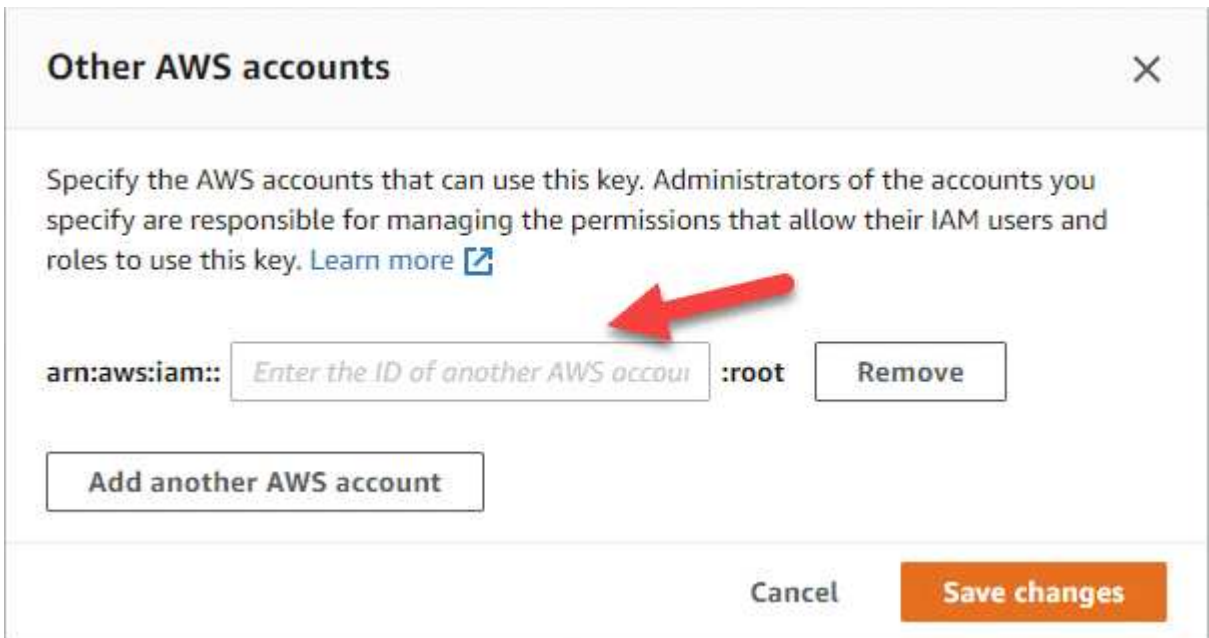
e. Now switch to the AWS account that provides Cloud Manager with permissions and open the IAM console.

f. Create an IAM policy that includes the permissions listed below.

g. Attach the policy to the IAM role or IAM user that provides permissions to Cloud Manager.

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

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

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

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

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

stored in the S3 bucket.

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

AWS Documentation: Editing Keys

Set up IAM roles for Cloud Volumes ONTAP

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

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

> ⓘ | Providing your own IAM role is required in the AWS Commercial Cloud Services Environment. Learn how to deploy Cloud Volumes ONTAP in C2S.

Steps

1. Go to the AWS IAM console.

2. Create an IAM policy that includes the following permissions:

   ◦ Cloud Volumes ONTAP nodes

Standard regions

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

GovCloud (US) regions

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

C2S environment

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

◦ HA mediator

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

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

Result

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

More information

- AWS documentation: Creating IAM policies

- AWS documentation: Creating IAM roles

Set up licensing for Cloud Volumes ONTAP in AWS

After you decide which licensing option you want to use with Cloud Volumes ONTAP, a few steps are required before you can choose that licensing option when creating a new working environment.

Freemium

Select the Freemium offering to use Cloud Volumes ONTAP free of charge with up to 500 GiB of provisioned capacity. Learn more about the Freemium offering.

Steps

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

   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the AWS Marketplace.

   You won't be charged through the marketplace subscription unless you exceed 500 GiB of provisioned capacity, at which time the system is automatically converted to the Essentials package.

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

View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

Capacity-based license

Capacity-based licensing enables you to pay for Cloud Volumes ONTAP per TiB of capacity. Capacity-based licensing is available in the form of a *package*: the Essentials package or the Professional package.

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

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

Learn more about capacity-based licensing.

The following sections describe how to get started with each of these consumption models.

BYOL

Pay upfront by purchasing a license (BYOL) from NetApp to deploy Cloud Volumes ONTAP systems in any cloud provider.

Steps

1. Contact NetApp Sales to obtain a license
2. Add your NetApp Support Site account to Cloud Manager

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

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

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

   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the AWS Marketplace.

   The license that you purchased from NetApp is always charged first, but you'll be charged from the hourly rate in the marketplace if you exceed your licensed capacity or if the term of your license expires.

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

View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

PAYGO subscription

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

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

Steps

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

   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the AWS Marketplace.

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

View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

> 💡 You can manage the AWS Marketplace subscriptions associated with your AWS accounts from the Settings > Credentials page. Learn how to manage your AWS accounts and subscriptions

Annual contract

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

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

Steps

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

   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the annual contract in the AWS Marketplace.

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

View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

Keystone Flex Subscription

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service. Learn more about Keystone Flex Subscriptions.

Steps

1. If you don't have a subscription yet, contact NetApp

2. Contact NetApp to authorize your Cloud Manager user account with one or more Keystone Flex Subscriptions.

3. After NetApp authorizes your account, link your subscriptions for use with Cloud Volumes ONTAP.

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

    a. Select the Keystone Flex Subscription charging method when prompted to choose a charging method.

View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

Launching Cloud Volumes ONTAP in AWS

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

Before you get started

You need the following to create a working environment.

- A Connector that's up and running.
  - You should have a Connector that is associated with your workspace.
  - You should be prepared to leave the Connector running at all times.
- An understanding of the configuration that you want to use.

  You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, see Planning your Cloud Volumes ONTAP configuration.

- An understanding of what's required to set up licensing for Cloud Volumes ONTAP.

  Learn how to set up licensing.

- DNS and Active Directory for CIFS configurations.

  For details, see Networking requirements for Cloud Volumes ONTAP in AWS.

Launching a single-node Cloud Volumes ONTAP system in AWS

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

About this task

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

Steps

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

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

Field	Description
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.

Field	Description
Add tags	AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Credentials	Choose the AWS credentials associated with the account where you want to deploy this system. You can also associate the AWS Marketplace subscription to use with this Cloud Volumes ONTAP system. Click **Add Subscription** to associate the selected credentials with a new AWS Marketplace subscription. The subscription can be for an annual contract or to pay for Cloud Volumes ONTAP at an hourly rate. Learn how to add additional AWS credentials to Cloud Manager.

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

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

(video)

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

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

   ◦ Learn more about Cloud Data Sense.

   ◦ Learn more about Cloud Backup.

   ◦ Learn more about Monitoring.

6. **Location & Connectivity**: Enter the network information that you recorded in the AWS worksheet.

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

Field	Description
VPC	If you have an AWS Outpost, you can deploy a single node Cloud Volumes ONTAP system in that Outpost by selecting the Outpost VPC. The experience is the same as any other VPC that resides in AWS.
Generated security group	If you let Cloud Manager generate the security group for you, you need to choose how you'll allow traffic: • If you choose **Selected VPC only**, the source for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option. • If you choose **All VPCs**, the source for inbound traffic is the 0.0.0.0/0 IP range.
Use existing security group	If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.

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

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

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

Learn how to set up the AWS KMS for Cloud Volumes ONTAP.

Learn more about supported encryption technologies.

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

   ◦ Learn about licensing options for Cloud Volumes ONTAP.

   ◦ Learn how to set up licensing.

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

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

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

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

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

    If you prefer to use your own policy, it must meet policy requirements for Cloud Volumes ONTAP nodes.

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

    > If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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

    Note the following:

    ◦ The disk type is for the initial volume (and aggregate). You can choose a different disk type for subsequent volumes (and aggregates).

    ◦ If you choose a gp3 or io1 disk, Cloud Manager uses the Elastic Volumes feature in AWS to automatically increase the underlying storage disk capacity as needed. You can choose the initial capacity based on your storage needs and revise it after Cloud Volumes ONTAP is deployed. Learn more about support for Elastic Volumes in AWS.

    ◦ If you choose a gp2 or st1 disk, you can select a disk size for all disks in the initial aggregate and for any additional aggregates that Cloud Manager creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

    ◦ You can choose a specific volume tiering policy when you create or edit a volume.

- ◦ If you disable data tiering, you can enable it on subsequent aggregates.

  [Learn how data tiering works](#).

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

    [Learn more about write speed](#).

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

    [Learn more about WORM storage](#).

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

    [Learn about supported client protocols and versions](#).

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

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.

Field	Description
Initiator group and IQN (for iSCSI only)	iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs. iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs). When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

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

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

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.

Field	Description
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager automation docs for details. Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

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

    For more information, see Understanding volume usage profiles and Data tiering overview.

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

    a. Review details about the configuration.

    b. Click **More information** to review details about support and the AWS resources that Cloud Manager will purchase.

    c. Select the **I understand…** check boxes.

    d. Click **Go**.

Result

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

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

For additional help, go to NetApp Cloud Volumes ONTAP Support.

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

- If you want to apply quotas to volumes, use System Manager or the CLI.

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

Launching a Cloud Volumes ONTAP HA pair in AWS

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

Limitation

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

About this task

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

Steps

1. On the Canvas page, click **Add Working Environment** and follow the prompts.

2. **Choose a Location**: Select **Amazon Web Services** and **Cloud Volumes ONTAP Single Node**.

3. **Details and Credentials**: Optionally change the AWS credentials and subscription, enter a working environment name, add tags if needed, and then enter a password.

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

Field	Description
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Add tags	AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Credentials	Choose the AWS credentials and marketplace subscription to use with this Cloud Volumes ONTAP system. Click **Add Subscription** to associate the selected credentials with a new AWS Marketplace subscription. The subscription can be for an annual contract or to pay for Cloud Volumes ONTAP at an hourly rate. If purchased a license directly from NetApp (BYOL), then an AWS subscription isn't required. Learn how to add additional AWS credentials to Cloud Manager.

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

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

(video)

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

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

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

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

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

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

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

Field	Description
Generated security group	If you let Cloud Manager generate the security group for you, you need to choose how you'll allow traffic: • If you choose **Selected VPC only**, the source for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option. • If you choose **All VPCs**, the source for inbound traffic is the 0.0.0.0/0 IP range.
Use existing security group	If you use an existing firewall policy, ensure that it includes the required rules. [Learn about firewall rules for Cloud Volumes ONTAP](#).

7. **Connectivity and SSH Authentication**: Choose connection methods for the HA pair and the mediator.

8. **Floating IPs**: If you chose multiple AZs, specify the floating IP addresses.

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

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

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

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

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

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

    Learn how to set up the AWS KMS for Cloud Volumes ONTAP.

    Learn more about supported encryption technologies.

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

    - Learn about licensing options for Cloud Volumes ONTAP.
    - Learn how to set up licensing.

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

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

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

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

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

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

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

    > ℹ️ If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

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

    Note the following:

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

more about support for Elastic Volumes in AWS.

- ◦ If you choose a gp2 or st1 disk, you can select a disk size for all disks in the initial aggregate and for any additional aggregates that Cloud Manager creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.
- ◦ You can choose a specific volume tiering policy when you create or edit a volume.
- ◦ If you disable data tiering, you can enable it on subsequent aggregates.

  Learn how data tiering works.

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

    Learn more about write speed.

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

    Learn more about WORM storage.

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

    Learn about supported client protocols and versions.

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

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.

Field	Description
Initiator group and IQN (for iSCSI only)	iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs. iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs). When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

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

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

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.

Field	Description
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager automation docs for details. Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

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

    For more information, see Understanding volume usage profiles and Data tiering overview.

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

    a. Review details about the configuration.

    b. Click **More information** to review details about support and the AWS resources that Cloud Manager will purchase.

    c. Select the **I understand…** check boxes.

    d. Click **Go**.

Result

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

If you experience any issues launching the HA pair, review the failure message. You can also select the working environment and click Re-create environment.

For additional help, go to NetApp Cloud Volumes ONTAP Support.

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

- If you want to apply quotas to volumes, use System Manager or the CLI.

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

Get started with Cloud Volumes ONTAP in the AWS C2S environment

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

region users.

Supported features in C2S

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

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

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

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

Limitations

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

Deployment overview

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

1. Preparing your AWS environment.

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

2. Installing the Connector and setting up Cloud Manager.

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

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

3. Launching Cloud Volumes ONTAP from Cloud Manager.

Each of these steps are described below.

Prepare your AWS environment

Your AWS environment must meet a few requirements.

Set up your networking

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

Steps

1. Choose the VPC and subnets in which you want to launch the Connector instance and Cloud Volumes ONTAP instances.

2. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.

3. Set up a VPC endpoint to the S3 service.

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

Subscribe to Cloud Volumes ONTAP

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

Steps

1. Go to the AWS Intelligence Community Marketplace and search for Cloud Volumes ONTAP.

2. Select the offering that you plan to deploy.

3. Review the terms and click **Accept**.

4. Repeat these steps for the other offerings, if you plan to deploy them.

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

Set up permissions

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

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

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

Steps

1. Go to the AWS IAM console and click **Policies**.

2. Create a policy for the Connector instance.

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

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

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

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

3. Create a policy for Cloud Volumes ONTAP.

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

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

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

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

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

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

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

Set up the AWS KMS

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

Steps

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

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

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

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

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

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

Install and set up Cloud Manager

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

Steps

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

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

2. Launch the Connector instance:

   a. Go to the AWS Intelligence Community Marketplace page for Cloud Manager.

   b. On the Custom Launch tab, choose the option to launch the instance from the EC2 console.

   c. Follow the prompts to configure the instance.

      Note the following as you configure the instance:

      ▪ We recommend t3.xlarge.

      ▪ You must choose the IAM role that you created when preparing your AWS environment.

      ▪ You should keep the default storage options.

      ▪ The required connection methods for the Connector are as follows: SSH, HTTP, and HTTPS.

3. Set up Cloud Manager from a host that has a connection to the Connector instance:

   a. Open a web browser and enter the following URL: http://ipaddress:80

   b. Specify a proxy server for connectivity to AWS services.

   c. Upload the certificate that you obtained in step 1.

   d. Complete the steps in the Setup wizard to set up Cloud Manager.

      ▪ **System Details**: Enter a name for this instance of Cloud Manager and provide your company name.

      ▪ **Create User**: Create the Admin user that you'll use to administer Cloud Manager.

      ▪ **Review**: Review the details and approve the end user license agreement.

   e. To complete installation of the CA-signed certificate, restart the Connector instance from the EC2 console.

4. After the Connector restarts, log in using the administrator user account that you created in the Setup wizard.

Launch Cloud Volumes ONTAP

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

What you'll need

• If you purchased a license, you must have the license file that you received from NetApp. The license file is a .NLF file in JSON format.

• A key pair is required to enable key-based SSH authentication to the HA mediator.

Steps

1. On the Working Environments page, click **Add Working Environment**.

2. Under Create, select Cloud Volumes ONTAP or Cloud Volumes ONTAP HA.

3. Complete the steps in the wizard to launch the Cloud Volumes ONTAP system.

   Note the following as you complete the wizard:

   ◦ If you want to deploy Cloud Volumes ONTAP HA in multiple Availability Zones, deploy the configuration as follows because only two AZs were available in the AWS Commercial Cloud Services environment at the time of publication:

     ▪ Node 1: Availability Zone A

     ▪ Node 2: Availability Zone B

     ▪ Mediator: Availability Zone A or B

   ◦ You should leave the default option to use a generated security group.

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

   ◦ You must choose the IAM role that you created when preparing your AWS environment.

   ◦ The underlying AWS disk type is for the initial Cloud Volumes ONTAP volume.

     You can choose a different disk type for subsequent volumes.

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

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

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

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

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

Result

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

Security group rules

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

Security group for the Connector

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

Inbound rules

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

Outbound rules

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

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

Security group for Cloud Volumes ONTAP

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

Inbound rules

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

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

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the System Manager web console using the IP address of the cluster management LIF
HTTPS	443	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos

Protocol	Port	Purpose
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
UDP	635	NFS mount
UDP	2049	NFS server daemon
UDP	4045	NFS lock daemon
UDP	4046	Network status monitor for NFS
UDP	4049	NFS rquotad protocol

Outbound rules

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

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

External security group for the HA mediator

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

Inbound rules

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

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

Outbound rules

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

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

Internal security group for the HA mediator

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

Inbound rules

The predefined security group includes the following inbound rules.

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

Outbound rules

The predefined security group includes the following outbound rules.

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

Use Cloud Volumes ONTAP

License management

Manage capacity-based licenses

Manage your capacity-based licenses from the Digital Wallet to ensure that your NetApp account has enough capacity for your Cloud Volumes ONTAP systems.

Capacity-based licenses enable you to pay for Cloud Volumes ONTAP per TiB of capacity.

The *Digital Wallet* enables you to manage licenses for Cloud Volumes ONTAP from a single location. You can add new licenses and update existing licenses.

Learn more about Cloud Volumes ONTAP licenses.

How licenses are added to the Digital Wallet

After you purchase a license from your NetApp sales representative, NetApp will send you an email with the serial number and additional licensing details.

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

If Cloud Manager can't add the license, you'll need to manually add them to the Digital Wallet yourself. For example, if the Connector is installed in a location that doesn't have internet access, you'll need to add the licenses yourself. Learn how to add purchased licenses to your account.

View the consumed capacity in your account

The Digital Wallet shows you the total consumed capacity in your account and the consumed capacity by licensing package. This can help you understand how you're being charged and whether you need to purchase additional capacity.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. With **Capacity Based Licenses** selected, view the packages summary, which shows you consumed capacity, total licensed capacity, and total PAYGO capacity.
   - *Total consumed capacity* is the total provisioned capacity of all Cloud Volumes ONTAP systems in your NetApp account. The charging is based on each volume's provisioned size, regardless of local, used, stored, or effective space within the volume.
   - *Total licensed* is the total licensed capacity (BYOL) that you purchased from NetApp.
   - *Total PAYGO* is the total provisioned capacity using cloud marketplace subscriptions. Charging via PAYGO is used only if the consumed capacity is higher than the licensed capacity or if there is no BYOL license available in the Digital Wallet.

     Here's an example of an account that has 2000 TiB of consumed capacity:

3. Under the summary, view the consumed capacity for each of your licensing packages.

   ◦ *Consumed capacity* shows you the total capacity of the volumes for that package. For more details about a specific package, hover your mouse over the tooltip.

     To better understand the capacities that display for the Essentials package, you should be familiar with how charging works. Learn about charging for the Essentials package.

   ◦ *BYOL* shows you the licensed capacity that you purchased from NetApp.

   ◦ *PAYGO* shows you the total consumed capacity by license consumption model.

     Here's an example for an account that has several licensing packages:

Add purchased licenses to your account

If you don't see your purchased licenses in the Digital Wallet, you'll need to add the licenses to Cloud Manager so that the capacity is available for Cloud Volumes ONTAP.

What you'll need

- You need to provide Cloud Manager the serial number of the license or the license file.
- If you want to enter the serial number, you first need to add your NetApp Support Site account to Cloud Manager. This is the NetApp Support Site account that's authorized to access the serial number.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, keep **Capacity Based Licenses** selected and click **Add License**.
3. Enter the serial number for your capacity-based license or upload the license file.

   If you entered a serial number, you also need to select the NetApp Support Site account that's authorized to access the serial number.

4. Click **Add License**.

Update a capacity-based license

If you purchased additional capacity or extended the term of your license, Cloud Manager automatically updates the license in the Digital Wallet. There's nothing that you need to do.

However, if you deployed Cloud Manager in a location that doesn't have internet access, then you'll need to manually update the license in Cloud Manager.

What you'll need

The license file (or *files* if you have an HA pair).

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. On the **Cloud Volumes ONTAP** tab, click the action menu next to the license and select **Update License**.

3. Upload the license file.

4. Click **Upload License**.

Change charging methods

You can change the charging method for a Cloud Volumes ONTAP system that uses capacity-based licensing. For example, if you deployed a Cloud Volumes ONTAP system with the Essentials package, you can change it to the Professional package if your business needs changed.

Important note

If you have a private offer or contract from your cloud provider's marketplace, changing to a charging method that's not included in your contract will result in charging against BYOL (if you purchased a license from NetApp) or PAYGO.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. On the **Cloud Volumes ONTAP** tab, click **Change Charging Method**.

3. Select a working environment, choose the new charging method, and then confirm your understanding that changing the package type will affect service charges.

4. Click **Change Charging Method**.

Result

Cloud Manager changes the charging method for the Cloud Volumes ONTAP system.

You might also notice that the Digital Wallet refreshes the consumed capacity for each package type to account for the change that you just made.

Remove a capacity-based license

If a capacity-based license expired and is no longer in use, then you can remove it at any time.

Steps
1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, click the action menu next to the license and select **Remove License**.
3. Click **Remove** to confirm.

Manage Keystone Flex Subscriptions

Manage your Keystone Flex Subscriptions from the Digital Wallet by enabling subscriptions for use with Cloud Volumes ONTAP. You can also request changes to the committed capacity and you can unlink subscriptions.

A *Keystone Flex Subscription* is a pay-as-you-grow storage service offered by NetApp.

The *Digital Wallet* enables you to manage licenses for Cloud Volumes ONTAP from a single location. You can add new licenses and update existing licenses.

Learn more about Cloud Volumes ONTAP licenses.

Authorize your account

Before you can use and manage Keystone Flex Subscriptions in Cloud Manager, you need to contact NetApp to authorize your Cloud Manager user account with your Keystone Flex Subscriptions.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. Click **Keystone Flex Subscription**.

3. If you see the **Welcome to NetApp Keystone** page, send an email to the address listed on the page.

   A NetApp representative will process your request by authorizing your user account to access the subscriptions.

4. Come back to the **Keystone Flex Subscription** to view your subscriptions.

What's next?
Link the subscriptions that you want to use with Cloud Volumes ONTAP.

Link a subscription

After NetApp authorizes your account, you need to link Keystone Flex Subscriptions for use with Cloud Volumes ONTAP. This action enables users to select the subscription as the charging method for new Cloud Volumes ONTAP systems.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. Click **Keystone Flex Subscription**.

3. For the subscription that you want to link, click ••• and select **Link**.

Result

The subscription is now linked to your Cloud Manager account and available to select when creating a Cloud Volumes ONTAP working environment.

Request more or less committed capacity

If you need to adjust the committed capacity for a subscription, you can send a request right from the Cloud Manager interface.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. Click **Keystone Flex Subscription**.

3. For the subscription that you want adjust the capacity, click ••• and select **View detail and edit**.

4. Enter the requested committed capacity for one or more subscriptions.

Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity	
Extreme	0.977 TiB	0.293 TiB	Enter amount	TiB
Premium	0.977 TiB	0.488 TiB	Enter amount	TiB
Performance	0 TiB	0 TiB	Enter amount	TiB
Standard	0.732 TiB	0.439 TiB	Enter amount	TiB
Value	0.977 TiB	⚠ 0.879 TiB	Enter amount	TiB
Data Tiering	0 TiB	0 TiB	Enter amount	TiB
CVO Primary	1.96 TiB	⚠ 1.76 TiB	3	TiB
CVO Secondary	1.02 TiB	0.488 TiB	Enter amount	TiB

Additional Information

Is there anything else we should know about your request?
Please be as descriptive as possible.

Enter your notes here

Submit   Cancel

5. Scroll down, enter any additional details for the request, and then click **Submit**.

Result

Your request creates a ticket in NetApp's system for processing.

Unlink a subscription

If you no longer want to use a Keystone Flex Subscription with new Cloud Volumes ONTAP systems, you can unlink the subscription. Note that you can only unlink a subscription that isn't attached to an existing Cloud Volumes ONTAP subscription.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. Click **Keystone Flex Subscription**.

3. For the subscription that you want to unlink, click ••• and select **Unlink**.

Result

The subscription is unlinked from your Cloud Manager account and no longer available to select when creating a Cloud Volumes ONTAP working environment.

Manage node-based licenses

Manage node-based licenses in the Digital Wallet to ensure that each Cloud Volumes ONTAP system has a valid license with the required capacity.

Node-based licenses are the previous generation licensing model (and not available for new customers):

- BYOL licenses purchased from NetApp
- Hourly pay-as-you-go (PAYGO) subscriptions from your cloud provider's marketplace

The *Digital Wallet* enables you to manage licenses for Cloud Volumes ONTAP from a single location. You can add new licenses and update existing licenses.

Learn more about Cloud Volumes ONTAP licenses.

Manage PAYGO licenses

The Digital Wallet page enables you to view details about each of your PAYGO Cloud Volumes ONTAP systems, including the serial number and PAYGO license type.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. Click **PAYGO**.
4. View details in the table about each of your PAYGO licenses.

5. If needed, click **Manage PAYGO License** to change the PAYGO license or to change the instance type.

Manage BYOL licenses

Manage licenses that you purchased directly from NetApp by adding and removing system licenses and extra capacity licenses.

Add unassigned licenses

Add a node-based license to the Digital Wallet so that you can select the license when you create a new Cloud Volumes ONTAP system. The Digital Wallet identifies these licenses as *unassigned*.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.

3. Click **Unassigned**.

4. Click **Add Unassigned Licenses**.

5. Enter the serial number of the license or upload the license file.

   If you don't have the license file yet, refer to the section below.

6. Click **Add License**.

Result

Cloud Manager adds the license to the Digital Wallet. The license will be identified as unassigned until you associate it with a new Cloud Volumes ONTAP system. After that happens, the license moves to the **BYOL** tab in the Digital Wallet.

Exchange unassigned node-based licenses

If you have an unassigned node-based license for Cloud Volumes ONTAP that you haven't used, you can exchange the license by converting it to a Cloud Backup license, a Cloud Data Sense license, or a Cloud Tiering license.

Exchanging the license revokes the Cloud Volumes ONTAP license and creates a dollar-equivalent license for the service:

- Licensing for a Cloud Volumes ONTAP HA pair is converted to a 51 TiB data service license
- Licensing for a Cloud Volumes ONTAP single node is converted to a 32 TiB data service license

The converted license has the same expiry date as the Cloud Volumes ONTAP license.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.

3. Click **Unassigned**.

4. Click **Exchange License**.

5. Select the service that you'd like to exchange the license with.

6. If you're prompted, select an additional license for the HA pair.

7. Read the legal consent and click **Agree**.

Result

Cloud Manager converts the unassigned license to the service that you selected. You can view the new license in the **Data Services Licenses** tab.

Obtain a system license file

In most cases, Cloud Manager can automatically obtain your license file using your NetApp Support Site account. But if it can't, then you'll need to manually upload the license file. If you don't have the license file, you can obtain it from netapp.com.

Steps

1. Go to the NetApp License File Generator and log in using your NetApp Support Site credentials.

2. Enter your password, choose your product, enter the serial number, confirm that you have read and accepted the privacy policy, and then click **Submit**.

   Example

3. Choose whether you want to receive the serialnumber.NLF JSON file through email or direct download.

Update a system license

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

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

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.

3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.

4. Click the action menu next to the system license and select **Update License**.

5. Upload the license file (or files if you have an HA pair).

6. Click **Update License**.

Result

Cloud Manager updates the license on the Cloud Volumes ONTAP system.

Manage extra capacity licenses

You can purchase extra capacity licenses for a Cloud Volumes ONTAP BYOL system to allocate more than the 368 TiB of capacity that's provided with a BYOL system license. For example, you might purchase one extra license capacity to allocate up to 736 TiB of capacity to Cloud Volumes ONTAP. Or you could purchase three extra capacity licenses to get up to 1.4 PiB.

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

Add capacity licenses

Purchase an extra capacity license by contacting us through the chat icon in the lower-right of Cloud Manager. After you purchase the license, you can apply it to a Cloud Volumes ONTAP system.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
4. Click **Add Capacity License**.
5. Enter the serial number or upload the license file (or files if you have an HA pair).
6. Click **Add Capacity License**.

Update capacity licenses

If you extended the term of an extra capacity license, you'll need to update the license in Cloud Manager.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
4. Click the action menu next to the capacity license and select **Update License**.
5. Upload the license file (or files if you have an HA pair).
6. Click **Update License**.

Remove capacity licenses

If an extra capacity license expired and is no longer in use, then you can remove it at any time.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.

4. Click the action menu next to the capacity license and select **Remove License**.

5. Click **Remove**.

Convert an Eval license to a BYOL

An evaluation license is good for 30 days. You can apply a new BYOL license on top of the evaluation license for an in-place upgrade.

When you convert an Eval license to a BYOL, Cloud Manager restarts the Cloud Volumes ONTAP system.

- For a single-node system, the restart results in I/O interruption during the reboot process.
- For an HA pair, the restart initiates takeover and giveback to continue serving I/O to clients.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.

3. Click **Eval**.

4. In the table, click **Convert to BYOL License** for a Cloud Volumes ONTAP system.

5. Enter the serial number or upload the license file.

6. Click **Convert License**.

Result

Cloud Manager starts the conversion process. Cloud Volumes ONTAP automatically restarts as part of this process. When it's back up, the licensing information will reflect the new license.

Change between PAYGO and BYOL

Converting a system from PAYGO by-node licensing to BYOL by-node licensing (and vice versa) isn't supported. If you want to switch between a pay-as-you-go subscription and a BYOL subscription, then you need to deploy a new system and replicate data from the existing system to the new system.

Steps

1. Create a new Cloud Volumes ONTAP working environment.

2. Set up a one-time data replication between the systems for each volume that you need to replicate.

   Learn how to replicate data between systems

3. Terminate the Cloud Volumes ONTAP system that you no longer need by deleting the original working environment.

   Learn how to delete a Cloud Volumes ONTAP working environment.

Volume and LUN administration

Create FlexVol volumes

If you need more storage after you launch your initial Cloud Volumes ONTAP system, you can create new FlexVol volumes for NFS, CIFS, or iSCSI from Cloud Manager.

Cloud Manager provides several ways to create a new volume:

- Specify details for a new volume and let Cloud Manager handle the underlying data aggregates for you. Learn more.
- Create a volume on a data aggregate of your choice. Learn more.
- Create volume from a template to optimize the volume for the workload requirements for certain applications, such as databases or streaming services. Learn more.
- Create a volume on the second node in an HA configuration. Learn more.

Before you get started

A few notes about volume provisioning:

- When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.
- You can create additional LUNs from System Manager or the CLI.
- If you want to use CIFS in AWS, you must have set up DNS and Active Directory. For details, see Networking requirements for Cloud Volumes ONTAP for AWS.
- If your Cloud Volumes ONTAP configuration supports the Amazon EBS Elastic Volumes feature, you might want to learn more about what happens when you create a volume.

Create a volume

The most common way to create a volume is to specify the type of volume that you need and then Cloud Manager handles the disk allocation for you. But you also have the option to choose the specific aggregate on which you want to create the volume.

Steps

1. On the Canvas page, double-click the name of the Cloud Volumes ONTAP system on which you want to provision a FlexVol volume.

2. Create a new volume by letting Cloud Manager handle the disk allocation for you, or choose a specific aggregate for the volume.

   Choosing a specific aggregate is recommended only if you have a good understanding of the data aggregates on your Cloud Volumes ONTAP system.

   Any aggregate

   In the Volumes tab, click **Add Volume** > **New volume**.

   Specific aggregate

   a. Click the menu icon, and then click **Advanced > Advanced allocation**.

   b. Click the menu for an aggregate.

   c. Click **Create volume**.

3. Follow the steps in the wizard to create the volume.

   a. **Details, Protection, and Tags**: Enter basic details about the volume and select a Snapshot policy.

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

Field	Description
Volume Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Tags	Tags that you add to a volume are associated with the Application Templates service, which can help you organize and simplify the management of your resources.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.

b. **Protocol**: Choose a protocol for the volume (NFS, CIFS, or iSCSI) and then provide the required information.

If you select CIFS and a server isn't set up, Cloud Manager prompts you to set up CIFS connectivity after you click **Next**.

Learn about supported client protocols and versions.

The following sections describe fields for which you might need guidance. The descriptions are organized by protocol.

NFS

Access control

Choose a custom export policy to make the volume available to clients.

Export policy

Defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.

CIFS

Permissions and users/groups

Enables you to control the level of access to an SMB share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.

DNS Primary and Secondary IP Address

The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.

Active Directory Domain to join

The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.

Credentials authorized to join the domain

The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.

CIFS server NetBIOS name

A CIFS server name that is unique in the AD domain.

Organizational Unit

The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.

- To configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=corp** in this field.

DNS Domain

The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

NTP Server

Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager automation docs for details.

Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

iSCSI

> **LUN**
>
> iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.
>
> **Initiator group**
>
> Initiator groups (igroups) specify which hosts can access specified LUNs on the storage system
>
> **Host initiator (IQN)**
>
> iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs).

 c. **Disk Type**: Choose an underlying disk type for the volume based on your performance needs and cost requirements.

  ▪ Sizing your system in AWS

 d. **Usage Profile & Tiering Policy**: Choose whether to enable or disable storage efficiency features on the volume and then select a volume tiering policy.

ONTAP includes several storage efficiency features that can reduce the total amount of storage that you need. NetApp storage efficiency features provide the following benefits:

Thin provisioning

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

Deduplication

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

Compression

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

 e. **Review**: Review details about the volume and then click **Add**.

Result

Cloud Manager creates the volume on the Cloud Volumes ONTAP system.

Create a volume from a template

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

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

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

Steps

1. On the Canvas page, click the name of the Cloud Volumes ONTAP system on which you want to provision a volume.

2. Click **⋮** > **Add Volume From Template**.

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

The *Define Parameters* page is displayed.

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

4. In the *Context* area, the Working Environment is filled in with the name of the working environment you started with. You need to select the **Storage VM** where the volume will be created.

5. Add values for all of the parameters that are not hard-coded from the template. See Create a volume for details about all the parameters you need to complete to deploy a Cloud Volumes ONTAP volume.

6. If there are no other Actions that you need to define (for example, configuring Cloud Backup), click **Run Template**.

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

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

7. Click **Run Template**.

Result

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

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

Create a volume on the second node in an HA configuration

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

Steps

1. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment on which you want to manage aggregates.

2. Click the menu icon and then click **Advanced > Advanced allocation**.

3. Click **Add Aggregate** and then create the aggregate.

4. For Home Node, choose the second node in the HA pair.

5. After Cloud Manager creates the aggregate, select it and then click **Create volume**.

6. Enter details for the new volume, and then click **Create**.

Result

Cloud Manager creates the volume on the second node in the HA pair.

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

After you create a volume

If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

If you want to apply quotas to volumes, you must use System Manager or the CLI. Quotas enable you to

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

Manage existing volumes

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

Manage volumes

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

Steps

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

Task	Action
View information about a volume	Select a volume, and then click **Info**.
Edit a volume (read-write volumes only)	a. Select a volume, and then click **Edit**. b. Modify the volume's Snapshot policy, NFS protocol version, NFS access control list (export policy), or share permissions, and then click **Update**. (i) If you need custom Snapshot policies, you can create them by using System Manager.
Clone a volume	a. Select a volume, and then click **Clone**. b. Modify the clone name as needed, and then click **Clone**. This process creates a FlexClone volume. A FlexClone volume is a writable, point-in-time copy that is space-efficient because it uses a small amount of space for metadata, and then only consumes additional space as data is changed or added. To learn more about FlexClone volumes, see the ONTAP 9 Logical Storage Management Guide.
Restore data from a Snapshot copy to a new volume	a. Select a volume, and then click **Restore from Snapshot copy**. b. Select a Snapshot copy, enter a name for the new volume, and then click **Restore**.
Create a Snapshot copy on demand	a. Select a volume, and then click **Create a Snapshot copy**. b. Change the name, if needed, and then click **Create**.

Task	Action
Get the NFS mount command	a. Select a volume, and then click **Mount Command**. b. Click **Copy**.
View the target iQN for an iSCSI volume	a. Select a volume, and then click **Target iQN**. b. Click **Copy**. c. Use the IQN to connect to the LUN from your hosts.
Change the underlying disk type	a. Select a volume, and then click **Change Disk Type & Tiering Policy**. b. Select the disk type, and then click **Change**. (i) Cloud Manager moves the volume to an existing aggregate that uses the selected disk type or it creates a new aggregate for the volume.
Change the tiering policy	a. Select a volume, and then click **Change Disk Type & Tiering Policy**. b. Click **Edit Policy**. c. Select a different policy and click **Change**. (i) Cloud Manager moves the volume to an existing aggregate that uses the selected disk type with tiering, or it creates a new aggregate for the volume.
Delete a volume	a. Select a volume, and then click **Delete**. b. Click **Delete** again to confirm.

Resize a volume

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

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

Modify the CIFS server

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

Steps

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

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

3. Click **Save**.

Result

Cloud Volumes ONTAP updates the CIFS server with the changes.

Move a volume

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

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

Steps

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

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

   For instructions, see the ONTAP 9 Volume Move Express Guide.

Move a volume when Cloud Manager displays an Action Required message

Cloud Manager might display an Action Required message that says moving a volume is necessary to avoid capacity issues, but that you need to correct the issue yourself. If this happens, you need to identify how to correct the issue and then move one or more volumes.

Cloud Manager displays these Action Required messages when an aggregate has reached 90% used capacity. If data tiering is enabled, the messages display when an aggregate has reached 80% used capacity. By default, 10% free space is reserved for data tiering. Learn more about the free space ratio for data tiering.

Steps

1. Identify how to correct the issue.

2. Based on your analysis, move volumes to avoid capacity issues:

   ◦ Move volumes to another system.

   ◦ Move volumes to another aggregate on the same system.

Identify how to correct capacity issues

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

Steps

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

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

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

   a. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.

   b. Select the aggregate, and then click **Info**.

   c. Expand the list of volumes.

   Used Aggregate Capacity: 105.66 GB

   Volumes: 4

   Vol54 (54 GB)

   data_vol (150 GB)

   svm_FinanceOnPrem_root (1 GB)

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

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

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

For details, see Moving volumes to another aggregate to avoid capacity issues.

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

   a. Delete any unused volumes.

   b. Rearrange volumes to free space on an aggregate.

      For details, see Moving volumes to another aggregate to avoid capacity issues.

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

      For details, see Moving volumes to another system to avoid capacity issues.

Move volumes to another system to avoid capacity issues

You can move one or more volumes to another Cloud Volumes ONTAP system to avoid capacity issues. You might need to do this if the system reached its disk limit.

About this task

You can follow the steps in this task to correct the following Action Required message:

```
Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
```

Steps

1. Identify a Cloud Volumes ONTAP system that has available capacity, or deploy a new system.

2. Drag and drop the source working environment on the target working environment to perform a one-time data replication of the volume.

   For details, see Replicating data between systems.

3. Go to the Replication Status page, and then break the SnapMirror relationship to convert the replicated volume from a data protection volume to a read/write volume.

   For details, see Managing data replication schedules and relationships.

4. Configure the volume for data access.

   For information about configuring a destination volume for data access, see the ONTAP 9 Volume Disaster Recovery Express Guide.

5. Delete the original volume.

   For details, see Manage volumes.

Move volumes to another aggregate to avoid capacity issues

You can move one or more volumes to another aggregate to avoid capacity issues.

About this task

You can follow the steps in this task to correct the following Action Required message:

> Moving two or more volumes is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you.

Steps

1. Verify whether an existing aggregate has available capacity for the volumes that you need to move:

    a. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.

    b. Select each aggregate, click **Info**, and then view the available capacity (aggregate capacity minus used aggregate capacity).

aggr1

Aggregate Capacity:	442.94 GB
Used Aggregate Capacity:	105.66 GB

2. If needed, add disks to an existing aggregate:

    a. Select the aggregate, and then click **Add disks**.

    b. Select the number of disks to add, and then click **Add**.

3. If no aggregates have available capacity, create a new aggregate.

    For details, see Creating aggregates.

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

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

    For instructions, see the ONTAP 9 Volume Move Express Guide.

Reasons why a volume move might perform slowly

Moving a volume might take longer than you expect if any of the following conditions are true for Cloud Volumes ONTAP:

- The volume is a clone.
- The volume is a parent of a clone.
- The source or destination aggregate has a single Throughput Optimized HDD (st1) disk.
- One of the aggregates uses an older naming scheme for objects. Both aggregates have to use the same name format.

    An older naming scheme is used if data tiering was enabled on an aggregate in the 9.4 release or earlier.

- The encryption settings don't match on the source and destination aggregates, or a rekey is in progress.

- The *-tiering-policy* option was specified on the volume move to change the tiering policy.

- The *-generate-destination-key* option was specified on the volume move.

Tiering inactive data to low-cost object storage

You can reduce storage costs for Cloud Volumes ONTAP by combining an SSD or HDD performance tier for hot data with an object storage capacity tier for inactive data. Data tiering is powered by FabricPool technology. For a high-level overview, see Data tiering overview.

To set up data tiering, you need to do the following:

1 **Choose a supported configuration**

Most configurations are supported. If you have a Cloud Volumes ONTAP system running the most recent version, then you should be good to go. Learn more.

2 **Ensure connectivity between Cloud Volumes ONTAP and object storage**

- For AWS, you'll need a VPC Endpoint to S3. Learn more.

3 **Ensure that you have an aggregate with tiering enabled**

Data tiering must be enabled on an aggregate in order to enable data tiering on a volume. You should be aware of the requirements for new volumes and for existing volumes. Learn more.

4 **Choose a tiering policy when creating, modifying, or replicating a volume**

Cloud Manager prompts you to choose a tiering policy when you create, modify, or replicate a volume.

- Tiering data on read-write volumes

- Tiering data on data protection volumes

> **What's not required for data tiering?**
>
> - You don't need to install a feature license to enable data tiering.
>
> - You don't need to create an object store for the capacity tier. Cloud Manager does that for you.
>
> - You don't need to enable data tiering at the system level.
>
>   Cloud Manager creates an object store for cold data when the system is created, as long as there are no connectivity or permissions issues. After that, you just need to enable data tiering on volumes (and in some cases, on aggregates).

Configurations that support data tiering

You can enable data tiering when using specific configurations and features.

Support in AWS

- Data tiering is supported in AWS starting with Cloud Volumes ONTAP 9.2.

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

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

Feature interoperability

- Data tiering is supported with encryption technologies.

- Thin provisioning must be enabled on volumes.

Requirements

Depending on your cloud provider, certain connections and permissions must be set up so that Cloud Volumes ONTAP can tier cold data to object storage.

Requirements to tier cold data to AWS S3

Ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, see AWS Documentation: Creating a Gateway Endpoint.

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

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

Enabling data tiering after implementing the requirements

Cloud Manager creates an object store for cold data when the system is created, as long as there are no connectivity or permissions issues. If you didn't implement the requirements listed above until after you created the system, then you'll need to manually enable tiering, which creates the object store.

Steps

1. Ensure that you've met all requirements.

2. On the Canvas page, double-click the name of the Cloud Volumes ONTAP instance.

3. Click the menu icon and select **Enable capacity tiering**.

You'll only see this option if data tiering couldn't be enabled when Cloud Manager created the system.

In Google Cloud, a service account must be attached to Cloud Volumes ONTAP before this option will appear. Ensure that you've met all requirements.

4. Click **Enable** so Cloud Manager can create the object store that this Cloud Volumes ONTAP system will use for tiered data.

Ensuring that tiering is enabled on aggregates

Data tiering must be enabled on an aggregate in order to enable data tiering on a volume. You should be aware of the requirements for new volumes and for existing volumes.

- **New volumes**

  If you're enabling data tiering on a new volume, then you don't need to worry about enabling data tiering on an aggregate. Cloud Manager creates the volume on an existing aggregate that has tiering enabled, or it creates a new aggregate for the volume if a data tiering-enabled aggregate doesn't already exist.

- **Existing volumes**

  If you want to enable data tiering on an existing volume, then you'll need to ensure that data tiering is enabled on the underlying aggregate. If data tiering isn't enabled on the existing aggregate, then you'll need to use System Manager to attach an existing aggregate to the object store.

Steps to confirm whether tiering is enabled on an aggregate

1. Open the working environment in Cloud Manager.

2. Click the menu icon, click **Advanced**, and then click **Advanced allocation**.

3. Verify whether tiering is enabled or disabled on the aggregate.

Steps to enable tiering on an aggregate

1. In System Manager, click **Storage > Tiers**.

2. Click the action menu for the aggregate and select **Attach Cloud Tiers**.

3. Select the cloud tier to attach and click **Save**.

What's next?

You can now enable data tiering on new and existing volumes, as explained in the next section.

Tiering data from read-write volumes

Cloud Volumes ONTAP can tier inactive data on read-write volumes to cost-effective object storage, freeing up the performance tier for hot data.

Steps

1. In the working environment, create a new volume or change the tier of an existing volume:

Task	Action
Create a new volume	Click **Add New Volume**.
Modify an existing volume	Select the volume and click **Change Disk Type & Tiering Policy**.

2. Select a tiering policy.

   For a description of these policies, see Data tiering overview.

   Example

Cloud Manager creates a new aggregate for the volume if a data tiering-enabled aggregate does not already exist.

Tiering data from data protection volumes

Cloud Volumes ONTAP can tier data from a data protection volume to a capacity tier. If you activate the destination volume, the data gradually moves to the performance tier as it is read.

Steps

1. On the Canvas page, select the working environment that contains the source volume, and then drag it to the working environment to which you want to replicate the volume.

2. Follow the prompts until you reach the tiering page and enable data tiering to object storage.

   Example

   For help with replicating data, see Replicating data to and from the cloud.

Changing the storage class for tiered data

After you deploy Cloud Volumes ONTAP, you can reduce your storage costs by changing the storage class for inactive data that hasn't been accessed for 30 days. The access costs are higher if you do access the data, so you must take that into consideration before you change the storage class.

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

For information about supported storage classes, see Data tiering overview.

Steps

1. From the working environment, click the menu icon and then click **Storage Classes** or **Blob Storage Tiering**.

2. Choose a storage class and then click **Save**.

Changing the free space ratio for data tiering

The free space ratio for data tiering defines how much free space is required on Cloud Volumes ONTAP SSDs/HDDs when tiering data to object storage. The default setting is 10% free space, but you can tweak the setting based on your requirements.

For example, you might choose less than 10% free space to ensure that you are utilizing the purchased capacity. Cloud Manager can then purchase additional disks for you when additional capacity is required (up until you reach the disk limit for the aggregate).

> ⚠ If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data and you might experience performance degradation. Any change should be done with caution. If you're unsure, reach out to NetApp support for guidance.

The ratio is important for disaster recovery scenarios because as data is read from the object store, Cloud Volumes ONTAP moves the data to SSDs/HDDs to provide better performance. If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data. Take this into consideration when changing the ratio so that you can meet your business requirements.

Steps

1. In the upper right of the Cloud Manager console, click the **Settings** icon, and select **Connector Settings**.

2. Under **Capacity**, click **Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering**.

3. Change the free space ratio based on your requirements and click **Save**.

Changing the cooling period for the auto tiering policy

If you enabled data tiering on a Cloud Volumes ONTAP volume using the *auto* tiering policy, you can adjust the default cooling period based on your business needs. This action is supported using the API only.

The cooling period is the number of days that user data in a volume must remain inactive before it is considered "cold" and moved to object storage.

The default cooling period for the auto tiering policy is 31 days. You can change the cooling period as follows:

- 9.8 or later: 2 days to 183 days

- 9.7 or earlier: 2 days to 63 days

Step

1. Use the *minimumCoolingDays* parameter with your API request when creating a volume or modifying an existing volume.

Connect a LUN to a host

When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

Note the following:

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

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

Steps

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

2. Select a volume, and then click **Target iQN**.

3. Click **Copy** to copy the iQN name.

4. Set up an iSCSI connection from the host to the LUN.

   - ONTAP 9 iSCSI express configuration for Red Hat Enterprise Linux: Starting the iSCSI sessions with the target

   - ONTAP 9 iSCSI express configuration for Windows: Starting iSCSI sessions with the target

Accelerate data access with FlexCache volumes

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

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

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

- FlexCache Volumes for Faster Data Access Power Guide

- Creating FlexCache volumes in System Manager

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

Aggregate administration

Create aggregates

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

> ⚠️ 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.

Steps

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

AWS

- If you're prompted to choose a disk type and disk size, refer to Plan your Cloud Volumes ONTAP configuration in AWS.

- If you're prompted to enter the aggregate's capacity size, then you're creating an aggregate on a configuration that supports the Amazon EBS Elastic Volumes feature. The following screenshot shows an example of a new aggregate comprised of gp3 disks.

Learn more about support for Elastic Volumes.

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

Manage aggregates

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

> ⚠️ 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.

Before you begin

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

About this task

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

Steps

1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage aggregates.

2. Click the menu icon and then click **Advanced > Advanced allocation**.

3. Manage your aggregates:

Task	Action
View information about an aggregate	Select an aggregate and click **Info**.
Create a volume on a specific aggregate	Select an aggregate and click **Create volume**.
Add disks to an aggregate	a. Select an aggregate and click **Add disks**. b. Select the number of disks that you want to add and click **Add**. 💡 All disks in an aggregate must be the same size.

Increase the capacity of an aggregate that supports Amazon EBS Elastic Volumes	a. Select an aggregate and click **Increase capacity**.
	
	b. Enter the additional capacity that you'd like to add and then click **Add**.
	
	   Note that you must increase the capacity of the aggregate by a minimum of 256 GiB or 10% of the aggregate's size.
	
	   For example, if you have a 1.77 TiB aggregate, 10% is 181 GiB. That's lower than 256 GiB, so the size of the aggregate must in increased by the 256 GiB minimum.

Delete an aggregate	a. Select an aggregate that does not contain any volumes and click **Delete**. b. Click **Delete** again to confirm.

Manage capacity settings on a Connector

Each Connector has settings that determines how it manages aggregate capacity for Cloud Volumes ONTAP.

These settings affect all Cloud Volumes ONTAP systems managed by a Connector. If you have another Connector, it can be configured differently.

Required permissions

Account Admin privileges are required to modify Connector settings.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.

2. Under **Capacity**, modify any of the following settings:

   Capacity Management Mode

   Choose whether Cloud Manager notifies you of storage capacity decisions or whether Cloud Manager automatically manages capacity requirements for you.

   Learn how Capacity Management Mode works.

Free Space Ratio

Triggers a notification when the free space ratio on an aggregate drops below the specified threshold.

The free space ratio is calculated as follows:

(aggregate capacity - total used capacity on the aggregate) / aggregate capacity

Free Space Ratio for Data Tiering

Defines how much free space is required on the performance tier (disks) when tiering data to a capacity tier (object storage).

The ratio is important for disaster recovery scenarios. As data is read from the capacity tier, Cloud Volumes ONTAP moves data to the performance tier to provide better performance. If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data.

3. Click **Save**.

Storage VM administration

Manage storage VMs in Cloud Manager

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but some configurations support additional storage VMs.

Supported number of storage VMs

Multiple storage VMs are supported with certain configurations. Go to the Cloud Volumes ONTAP Release Notes to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

Work with multiple storage VMs

Cloud Manager supports any additional storage VMs that you create from System Manager or the CLI.

For example, the following image shows how you can choose a storage VM when you create a volume.

And the following image shows how you can choose a storage VM when replicating a volume to another system.

Modify the name of the default storage VM

Cloud Manager automatically names the single storage VM that it creates for Cloud Volumes ONTAP. You can modify the name of the storage VM if you have strict naming standards. For example, you might want the name to match how you name the storage VMs for your ONTAP clusters.

If you created any additional storage VMs for Cloud Volumes ONTAP, then you can't rename the storage VMs from Cloud Manager. You'll need to do so directly from Cloud Volumes ONTAP by using System Manager or

the CLI.

Steps

1. From the working environment, click the menu icon, and then click **Information**.

2. Click the edit icon to the right of the storage VM name.

3. In the Modify SVM Name dialog box, change the name, and then click **Save**.

Manage storage VMs for disaster recovery

Cloud Manager doesn't provide any setup or orchestration support for storage VM disaster recovery. You must use System Manager or the CLI.

- SVM Disaster Recovery Preparation Express Guide
- SVM Disaster Recovery Express Guide

Create data-serving storage VMs for Cloud Volumes ONTAP in AWS

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but some configurations support additional storage VMs.

To create additional data-serving storage VMs, you need to allocate IP addresses in AWS and then run ONTAP commands based on your Cloud Volumes ONTAP configuration.

Supported number of storage VMs

Multiple storage VMs are supported with specific Cloud Volumes ONTAP configurations starting with the 9.7 release. Go to the Cloud Volumes ONTAP Release Notes to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All other Cloud Volumes ONTAP configurations support one data-serving storage VM and one destination storage VM used for disaster recovery. You can activate the destination storage VM for data access if there's an outage on the source storage VM.

Verify limits for your configuration

Each EC2 instance supports a maximum number of private IPv4 addresses per network interface. You need to verify the limit before you allocate IP addresses in AWS for the new storage VM.

Steps

1. Go the Storage limits section in the Cloud Volumes ONTAP Release Notes.

2. Identify the maximum number of IP addresses per interface for your instance type.

3. Make note of this number because you'll need it in the next section when you allocate IP addresses in AWS.

Allocate IP addresses in AWS

Private IPv4 addresses must be assigned to port e0a in AWS before you create LIFs for the new storage VM.

Note that an optional management LIF for a storage VM requires a private IP address on a single node system and on an HA pair in a single AZ. This management LIF provides a connection to management tools like SnapCenter.

Steps

1. Log in to AWS and open the EC2 service.

2. Select the Cloud Volumes ONTAP instance and click **Networking**.

   If you're creating a storage VM on an HA pair, select node 1.

3. Scroll down to **Network interfaces** and click the **Interface ID** for port e0a.
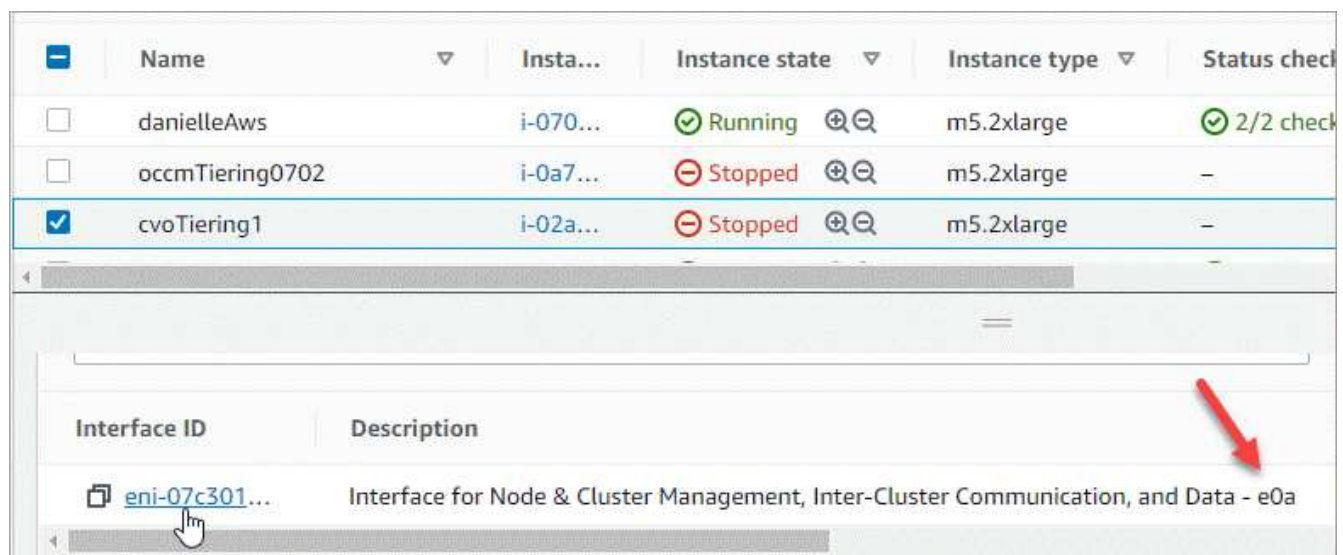
4. Select the network interface and click **Actions > Manage IP addresses**.

5. Expand the list of IP addresses for e0a.

6. Verify the IP addresses:

   a. Count the number of allocated IP addresses to confirm that the port has room for additional IPs.

      You should have identified the maximum number of supported IP addresses per interface in the previous section of this page.

   b. Optional: Go to the CLI for Cloud Volumes ONTAP and run **network interface show** to confirm that each of these IP addresses are in use.

      If an IP address isn't in use, then you can use it with the new storage VM.

7. Back in the AWS Console, click **Assign new IP address** to assign additional IP addresses based on the amount that you need for the new storage VM.

   ◦ Single node system: One unused secondary private IP is required.

      An optional secondary private IP is required if you want to create a management LIF on the storage VM.

   ◦ HA pair in a single AZ: One unused secondary private IP is required on node 1.

      An optional secondary private IP is required if you want to create a management LIF on the storage VM.

   ◦ HA pair in multiple AZs: One unused secondary private IP is required on each node.

8. If you're allocating the IP address on an HA pair in a single AZ, enable **Allow secondary private IPv4 addresses to be reassigned**.

9. Click **Save**.

10. If you have an HA pair in multiple AZs, then you'll need to repeat these steps for node 2.

Create a storage VM on a single node system

These steps create a new storage VM on a single node system. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

Steps

1. Create the storage VM and a route to the storage VM.

   ```
   vserver create -rootvolume-security-style unix -rootvolume root_svm_2
   -snapshot-policy default -vserver svm_2 -aggregate aggr1
   ```

   ```
   network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
   subnet_gateway
   ```

2. Create a NAS LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node
```

Where *private_ip_x* is an unused secondary private IP on e0a.

3. Optional: Create a storage VM management LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

Where *private_ip_y* is another unused secondary private IP on e0a.

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

Create a storage VM on an HA pair in a single AZ

These steps create a new storage VM on an HA pair in a single AZ. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

Both of these LIFs get allocated on node 1. The private IP addresses can move between nodes if failures occur.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

Where *private_ip_x* is an unused secondary private IP on e0a of cvo-node1. This IP address can be relocated to the e0a of cvo-node2 in case of takeover because the service policy default-data-files indicates that IPs can migrate to the partner node.

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

Where *private_ip_y* is another unused secondary private IP on e0a.

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

5. If you're running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Create a storage VM on an HA pair in multiple AZs

These steps create a new storage VM on an HA pair in multiple AZs.

A *floating* IP address is required for a NAS LIF and is optional for a management LIF. These floating IP addresses don't require you to allocate private IPs in AWS. Instead, the floating IPs are automatically configured in the AWS route table to point to a specific node's ENI in the same VPC.

In order for floating IPs to work with ONTAP, a private IP address must be configured on every storage VM on each node. This is reflected in the steps below where an iSCSI LIF is created on node 1 and on node 2.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

   ◦ The floating IP address must be outside of the CIDR blocks for all VPCs in the AWS region in which
     you deploy the HA configuration. 192.168.209.27 is an example floating IP address. Learn more about
     choosing a floating IP address.

   ◦ `-service-policy default-data-files` indicates that IPs can migrate to the partner node.

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. Create an iSCSI LIF on node 1.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

   ◦ This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have
     to be an iSCSI LIF, but it can't be configured to migrate between nodes.

   ◦ `-service-policy default-data-block` indicates that an IP address does not migrate between
     nodes.

   ◦ *private_ip* is an unused secondary private IP address on eth0 (e0a) of cvo_node1.

5. Create an iSCSI LIF on node 2.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

- This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
- `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.
- *private_ip* is an unused secondary private IP address on eth0 (e0a) of cvo_node2.

6. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

7. If you're running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Security and data encryption

Encrypting volumes with NetApp encryption solutions

Cloud Volumes ONTAP supports NetApp Volume Encryption (NVE) and NetApp
Aggregate Encryption (NAE). NVE and NAE are software-based solutions that enable
FIPS 140-2–compliant data-at-rest encryption of volumes. Learn more about these
encryption solutions.

Both NVE and NAE are supported with an external key manager.

New aggregates will have NAE enabled by default after you set up an external key manager. New volumes that
aren't part of an NAE aggregate will have NVE enabled by default (for example, if you have existing
aggregates that were created before setting up an external key manager).

Cloud Volumes ONTAP doesn't support onboard key management.

What you'll need

Your Cloud Volumes ONTAP system should be registered with NetApp support. A NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support.

- Adding NetApp Support Site accounts to Cloud Manager
- Registering pay-as-you-go systems

ⓘ Cloud Manager doesn't install the NVE license on systems that reside in the China region.

Steps

1. Review the list of supported key managers in the NetApp Interoperability Matrix Tool.

   💡 Search for the **Key Managers** solution.

2. Connect to the Cloud Volumes ONTAP CLI.

3. Configure external key management.
   - AWS: Go to the ONTAP documentation for instructions

Improving protection against ransomware

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

Using this feature to improve protection against ransomware addresses a separate use case from the ONTAP anti-ransomware feature that you can enable through System Manager or the ONTAP CLI.

Steps

1. From the working environment, click the **Ransomware** icon.
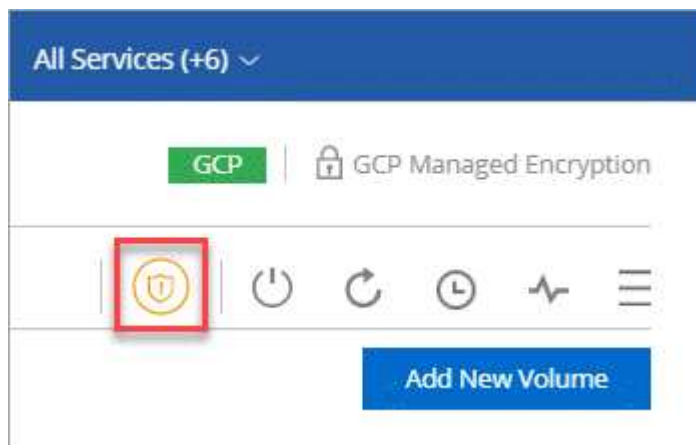
2. Implement the NetApp solution for ransomware:

   a. Click **Activate Snapshot Policy**, if you have volumes that do not have a Snapshot policy enabled.

NetApp Snapshot technology provides the industry's best solution for ransomware remediation. The key to a successful recovery is restoring from uninfected backups. Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

b. Click **Activate FPolicy** to enable ONTAP's FPolicy solution, which can block file operations based on a file's extension.

This preventative solution improves protection from ransomware attacks by blocking common ransomware file types.

The default FPolicy scope blocks files that have the following extensions:

micro, encrypted, locked, crypto, crypt, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, good, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre

> Cloud Manager creates this scope when you activate FPolicy on Cloud Volumes ONTAP. The list is based on common ransomware file types. You can customize the blocked file extensions by using the *vserver fpolicy policy scope* commands from the Cloud Volumes ONTAP CLI.

System administration

Upgrade Cloud Volumes ONTAP software

Upgrade Cloud Volumes ONTAP from Cloud Manager to gain access to the latest new features and enhancements. You should prepare Cloud Volumes ONTAP systems before you upgrade the software.

Upgrade overview

You should be aware of the following before you start the Cloud Volumes ONTAP upgrade process.

Upgrade from Cloud Manager only

Upgrades of Cloud Volumes ONTAP must be completed from Cloud Manager. You should not upgrade Cloud Volumes ONTAP by using System Manager or the CLI. Doing so can impact system stability.

How to upgrade

Cloud Manager provides two ways to upgrade Cloud Volumes ONTAP:

- By following upgrade notifications that appear in the working environment
- By placing the upgrade image at an HTTPS location and then providing Cloud Manager with the URL

Supported upgrade paths

The version of Cloud Volumes ONTAP that you can upgrade to depends on the version of Cloud Volumes ONTAP that you're currently running.

Current version	Versions that you can directly upgrade to
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Note the following:

- The supported upgrade paths for Cloud Volumes ONTAP are different than they are for an on-premises ONTAP cluster.
- If you upgrade by following the upgrade notifications that appear in a working environment, Cloud Manager will prompt you to upgrade to a release that follows these supported upgrade paths.

- If you upgrade by placing an upgrade image at an HTTPS location, be sure to follow these supported upgrade paths.

- In some cases, you might need to upgrade a few times to reach your target release.

  For example, if you're running version 9.8 and you want to upgrade to 9.10.1, you first need to upgrade to version 9.9.1 and then to 9.10.1.

Reverting or downgrading

Reverting or downgrading Cloud Volumes ONTAP to a previous release is not supported.

Support registration

Cloud Volumes ONTAP must be registered with NetApp support in order to upgrade the software using any of the methods described on this page. This applies to both PAYGO and BYOL. You'll need to manually register PAYGO systems, while BYOL systems are registered by default.

> A system that isn't registered for support will still receive the software update notifications that appear in Cloud Manager when a new version is available. But you will need to register the system before you can upgrade the software.

Upgrades of the HA mediator

Cloud Manager also updates the mediator instance as needed during the Cloud Volumes ONTAP upgrade process.

Prepare to upgrade

Before performing an upgrade, you must verify that your systems are ready and make any required configuration changes.

- Plan for downtime
- Verify that automatic giveback is still enabled
- Suspend SnapMirror transfers
- Verify that aggregates are online

Plan for downtime

When you upgrade a single-node system, the upgrade process takes the system offline for up to 25 minutes, during which I/O is interrupted.

Upgrading an HA pair is nondisruptive and I/O is uninterrupted. During this nondisruptive upgrade process, each node is upgraded in tandem to continue serving I/O to clients.

Verify that automatic giveback is still enabled

Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

ONTAP 9 Documentation: Commands for configuring automatic giveback

Suspend SnapMirror transfers

If a Cloud Volumes ONTAP system has active SnapMirror relationships, it is best to suspend transfers before you update the Cloud Volumes ONTAP software. Suspending the transfers prevents SnapMirror failures. You must suspend the transfers from the destination system.

> ℹ️ Even though Cloud Backup uses an implementation of SnapMirror to create backup files (called SnapMirror Cloud), backups do not need to be suspended when a system is upgraded.

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. Log in to System Manager from the destination system.

   You can log in to System Manager by pointing your web browser to the IP address of the cluster management LIF. You can find the IP address in the Cloud Volumes ONTAP working environment.

   > ℹ️ The computer from which you are accessing Cloud Manager must have a network connection to Cloud Volumes ONTAP. For example, you might need to log in to Cloud Manager from a jump host that's in your cloud provider network.

2. Click **Protection > Relationships**.
3. Select the relationship and click **Operations > Quiesce**.

Verify that aggregates are online

Aggregates for Cloud Volumes ONTAP must be online before you update the software. Aggregates should be online in most configurations, but if they are not, then you should bring them online.

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
2. Select an aggregate, click **Info**, and then verify that the state is online.

aggr1

Aggregate Capacity:	88.57 GB
Used Aggregate Capacity:	1.07 GB
Volumes:	2 ⌄
AWS Disks:	1 ⌄
State:	online

3. If the aggregate is offline, use System Manager to bring the aggregate online:

    a. Click **Storage > Aggregates & Disks > Aggregates**.

    b. Select the aggregate, and then click **More Actions > Status > Online**.

Upgrade Cloud Volumes ONTAP

Cloud Manager notifies you when a new version is available for upgrade. You can start the upgrade process from this notification. For details, see Upgrade from Cloud Manager notifications.

Another way to perform software upgrades by using an image on an external URL. This option is helpful if Cloud Manager can't access the S3 bucket to upgrade the software or if you were provided with a patch. For details, see Upgrade from an image available at a URL.

Upgrade from Cloud Manager notifications

Cloud Manager displays a notification in Cloud Volumes ONTAP working environments when a new version of Cloud Volumes ONTAP is available:

You can start the upgrade process from this notification, which automates the process by obtaining the software image from an S3 bucket, installing the image, and then restarting the system.

Before you begin

Cloud Manager operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.

Steps

1. From the left navigation menu, select **Canvas**.

2. Select a working environment.

   A notification appears in the right pane if a new version is available:

3. If a new version is available, click **Upgrade**.

4. In the Release Information page, click the link to read the Release Notes for the specified version, and then select the **I have read…** check box.

5. In the End User License Agreement (EULA) page, read the EULA, and then select **I read and approve the EULA**.

6. In the Review and Approve page, read the important notes, select **I understand…**, and then click **Go**.

Result

Cloud Manager starts the software upgrade. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

Upgrade from an image available at a URL

You can place the Cloud Volumes ONTAP software image on the Connector or on an HTTP server and then initiate the software upgrade from Cloud Manager. You might use this option if Cloud Manager can't access the S3 bucket to upgrade the software.

Before you begin

Cloud Manager operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.

Steps

1. Optional: Set up an HTTP server that can host the Cloud Volumes ONTAP software image.

If you have a VPN connection to the virtual network, you can place the Cloud Volumes ONTAP software

image on an HTTP server in your own network. Otherwise, you must place the file on an HTTP server in the cloud.

2. If you use your own security group for Cloud Volumes ONTAP, ensure that the outbound rules allow HTTP connections so Cloud Volumes ONTAP can access the software image.

> ⓘ The predefined Cloud Volumes ONTAP security group allows outbound HTTP connections by default.

3. Obtain the software image from the NetApp Support Site.

4. Copy the software image to a directory on the Connector or on an HTTP server from which the file will be served.

   For example, you can copy the software image to the following path on the Connector:

   `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`

5. From the working environment in Cloud Manager, click the menu icon, and then click **Advanced > Update Cloud Volumes ONTAP**.

6. On the update software page, enter the URL, and then click **Change Image**.

   If you copied the software image to the Connector in the path shown above, you would enter the following URL:

   http://<Connector-private-IP-address>/ontap/images/<image-file-name>

7. Click **Proceed** to confirm.

Result

Cloud Manager starts the software update. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

Registering pay-as-you-go systems

Support from NetApp is included with Cloud Volumes ONTAP PAYGO systems, but you must first activate support by registering the systems with NetApp.

Registering a PAYGO system with NetApp is required to upgrade ONTAP software using any of the methods described on this page.

> 💡 A system that isn't registered for support will still receive the software update notifications that appear in Cloud Manager when a new version is available. But you will need to register the system before you can upgrade the software.

Steps

1. If you have not yet added your NetApp Support Site account to Cloud Manager, go to **Account Settings** and add it now.

   Learn how to add NetApp Support Site accounts.

2. On the Canvas page, double-click the name of the system that you want to register.

3. Click the menu icon and then click **Support registration**:

4. Select a NetApp Support Site account and click **Register**.

Result

Cloud Manager registers the system with NetApp.

Managing the state of Cloud Volumes ONTAP

You can stop and start Cloud Volumes ONTAP from Cloud Manager to manage your cloud compute costs.

Scheduling automatic shutdowns of Cloud Volumes ONTAP

You might want to shut down Cloud Volumes ONTAP during specific time intervals to lower your compute costs. Rather than do this manually, you can configure Cloud Manager to automatically shut down and then restart systems at specific times.

About this task

- When you schedule an automatic shutdown of your Cloud Volumes ONTAP system, Cloud Manager postpones the shutdown if an active data transfer is in progress.

  Cloud Manager shuts down the system after the transfer is complete.

- This task schedules automatic shutdowns of both nodes in an HA pair.

- Snapshots of boot and root disks are not created when turning off Cloud Volumes ONTAP through scheduled shutdowns.

  Snapshots are automatically created only when performing a manual shutdown, as described in the next section.

Steps

1. From the working environment, click the clock icon:

2. Specify the shutdown schedule:

   a. Choose whether you want to shut down the system every day, every weekday, every weekend, or any combination of the three options.

   b. Specify when you want to turn off the system and for how long you want it turned off.

   Example

   The following image shows a schedule that instructs Cloud Manager to shut down the system every Saturday at 12:00 a.m. for 48 hours. Cloud Manager restarts the system every Monday at 12:00 a.m.

☐ **Turn off every weekday** Mon, Tue, Wed, Thu, Fri	turn off at 08 : 00 PM	for 12	Hours (1-24)
☑ **Turn off every weekend** Sat	turn off at 12 : 00 AM	for 48	Hours (1-48)

3. Click **Save**.

Result

Cloud Manager saves the schedule. The clock icon changes to indicate that a schedule is set:

Stopping Cloud Volumes ONTAP

Stopping Cloud Volumes ONTAP saves you from accruing compute costs and creates snapshots of the root and boot disks, which can be helpful for troubleshooting.

> ⓘ To reduce costs, Cloud Manager periodically deletes older snapshots of root and boot disks. Only the two most recent snapshots are retained for both the root and boot disks.

About this task

When you stop an HA pair, Cloud Manager shuts down both nodes.

Steps

1. From the working environment, click the **Turn off** icon.

2. Keep the option to create snapshots enabled because the snapshots can enable system recovery.

3. Click **Turn Off**.

   It can take up to a few minutes to stop the system. You can restart systems at a later time from the working environment page.

Synchronize the system time using NTP

Specifying an NTP server synchronizes the time between the systems in your network, which can help prevent issues due to time differences.

Specify an NTP server using the Cloud Manager API or from the user interface when you create a CIFS server.

Modify system write speed

Cloud Manager enables you to choose a normal or high write speed for Cloud Volumes ONTAP. The default write speed is normal. You can change to high write speed if fast write performance is required for your workload.

High write speed is supported with all types of single node systems and some HA pair configurations. View supported configurations in the Cloud Volumes ONTAP Release Notes

Before you change the write speed, you should understand the differences between the normal and high settings.

About this task

- Ensure that operations such as volume or aggregate creation are not in progress.
- Be aware that this change restarts the Cloud Volumes ONTAP system. This is disruptive process that requires downtime for the entire system.

Steps

1. From the working environment, click the menu icon, and then click **Advanced > Writing Speed**.
2. Select **Normal** or **High**.

   If you choose High, then you'll need to read the "I understand…" statement and confirm by checking the box.

3. Click **Save**, review the confirmation message, and then click **Proceed**.

Change the password for Cloud Volumes ONTAP

Cloud Volumes ONTAP includes a cluster admin account. You can change the password for this account from Cloud Manager, if needed.

> ⚠ You should not change the password for the admin account through System Manager or the CLI. The password will not be reflected in Cloud Manager. As a result, Cloud Manager cannot monitor the instance properly.

Steps

1. From the working environment, click the menu icon, and then click **Advanced > Set password**.
2. Enter the new password twice and then click **Save**.

   The new password must be different than one of the last six passwords that you used.

Add, remove, or delete systems

Adding existing Cloud Volumes ONTAP systems to Cloud Manager

You can discover and add existing Cloud Volumes ONTAP systems to Cloud Manager. You might do this if you deployed a new Cloud Manager system.

Before you begin
You must know the password for the Cloud Volumes ONTAP admin user account.

Steps

1. On the Canvas page, click **Add Working Environment**.
2. Select the cloud provider in which the system resides.
3. Choose the type of Cloud Volumes ONTAP system.
4. Click the link to discover an existing system.

5. On the Region page, choose the region where the instances are running, and then select the instances.
6. On the Credentials page, enter the password for the Cloud Volumes ONTAP admin user, and then click **Go**.

Result
Cloud Manager adds the Cloud Volumes ONTAP instances to the workspace.

Removing Cloud Volumes ONTAP working environments

The Account Admin can remove a Cloud Volumes ONTAP working environment to move it to another system or to troubleshoot discovery issues.

About this task

Removing a Cloud Volumes ONTAP working environment removes it from Cloud Manager. It does not delete the Cloud Volumes ONTAP system. You can later rediscover the working environment.

Removing a working environment from Cloud Manager enables you to do the following:

- Rediscover it in another workspace
- Rediscover it from another Cloud Manager system
- Rediscover it if you had problems during the initial discovery

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Tools**.

2. From the Tools page, click **Launch**.
3. Select the Cloud Volumes ONTAP working environment that you want to remove.
4. On the Review and Approve page, click **Go**.

Result

Cloud Manager removes the working environment. Users can rediscover this working environment from the Canvas page at any time.

Deleting a Cloud Volumes ONTAP system

You should always delete Cloud Volumes ONTAP systems from Cloud Manager, rather than from your cloud provider's console. For example, if you terminate a licensed Cloud Volumes ONTAP instance from your cloud provider, then you can't use the license key for another instance. You must delete the working environment from Cloud Manager to release the license.

When you delete a working environment, Cloud Manager terminates Cloud Volumes ONTAP instances and deletes disks and snapshots.

Resources managed by other services like backups for Cloud Backup and instances for Cloud Data Sense and Monitoring are not deleted when you delete a working environment. You'll need to manually delete them yourself. If you don't, then you'll continue to receive charges for these resources.

> ⓘ When Cloud Manager deploys Cloud Volumes ONTAP in your cloud provider, it enables termination protection on the instances. This option helps prevent accidental termination.

Steps

1. If you enabled Cloud Backup on the working environment, determine whether the backed up data is still required and then delete the backups, if necessary.

   Cloud Backup is independent from Cloud Volumes ONTAP by design. Cloud Backup doesn't automatically delete backups when you delete a Cloud Volumes ONTAP system, and there is no current support in the UI to delete the backups after the system has been deleted.

2. If you enabled Cloud Data Sense or Monitoring on this working environment and no other working environments use those services, then you'll need to delete the instances for those services.

   ◦ Learn more about the Cloud Data Sense instance.

   ◦ Learn more about the Monitoring Acquisition Unit.

3. Delete the Cloud Volumes ONTAP working environment.

   a. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment that you want to delete.

   b. Click menu icon and then click **Delete**.

   c. Type the name of the working environment and then click **Delete**.

   It can take up to 5 minutes to delete the working environment.

AWS administration

Change the EC2 instance type for Cloud Volumes ONTAP

You can choose from several instance or types when you launch Cloud Volumes ONTAP in AWS. You can change the instance type at any time if you determine that it is undersized or oversized for your needs.

About this task

• Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

ONTAP 9 Documentation: Commands for configuring automatic giveback

- Changing the instance type can affect AWS service charges.
- The operation restarts Cloud Volumes ONTAP.

  For single node systems, I/O is interrupted.

  For HA pairs, the change is nondisruptive. HA pairs continue to serve data.

  > Cloud Manager gracefully changes one node at a time by initiating takeover and waiting for give back. NetApp's QA team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, we did see retries on the I/O level, but the application layer overcame these short "re-wire" of NFS/CIFS connections.

Steps

1. From the working environment, click the menu icon, and then select **Change instance**.
2. If you are using a node-based PAYGO license, you can optionally choose a different license.
3. Choose an instance type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

Result

Cloud Volumes ONTAP reboots with the new configuration.

Change route tables for HA pairs in multiple AZs

You can modify the AWS route tables that include routes to the floating IP addresses for an HA pair that's deployed in multiple AWS Availability Zones (AZs). You might do this if new NFS or CIFS clients need to access an HA pair in AWS.

Steps

1. From the working environment, click the menu icon and then click **Information**.
2. Click **Route Tables**.
3. Modify the list of selected route tables and then click **Save**.

Result

Cloud Manager sends an AWS request to modify the route tables.

Monitoring AWS resource costs

Cloud Manager enables you to view the resource costs associated with running Cloud Volumes ONTAP in AWS. You can also see how much money you saved by using NetApp features that can reduce storage costs.

About this task

Cloud Manager updates the costs when you refresh the page. You should refer to AWS for final cost details.

Step

1. Verify that Cloud Manager can obtain cost information from AWS:
   a. Ensure that the IAM policy that provides Cloud Manager with permissions includes the required permissions.

b. Activate the **WorkingEnvironmentId** tag.

To track your AWS costs, Cloud Manager assigns a cost allocation tag to Cloud Volumes ONTAP instances. After you create your first working environment, activate the **WorkingEnvironmentId** tag. User-defined tags don't appear on AWS billing reports until you activate them in the Billing and Cost Management console.

2. On the Canvas page, select a Cloud Volumes ONTAP working environment and then click **Cost**.

The Cost page displays costs for the current and previous months and shows your annual NetApp savings, if you enabled NetApp's cost-saving features on volumes.

The following image shows a sample Cost page:
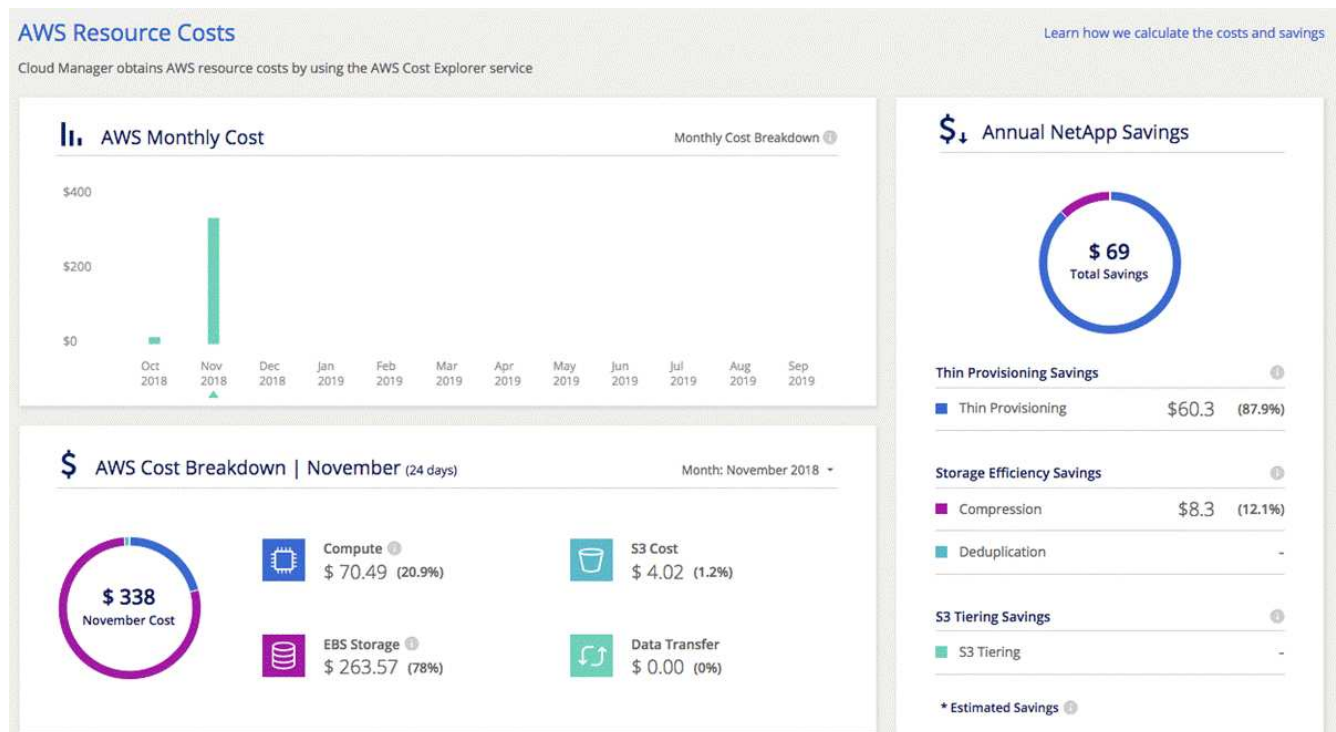
Administer Cloud Volumes ONTAP using the Advanced View

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using ONTAP System Manager, which is a management interface that's provided with an ONTAP system. We have included the System Manager interface directly inside Cloud Manager so that you don't need to leave Cloud Manager for advanced management.

This Advanced View is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Features

The Advanced View in Cloud Manager gives you access to additional management features:

- Advanced storage management

  Manage consistency groups, shares, qtrees, quotas, and Storage VMs.

- Networking management

  Manage IPspaces, network interfaces, portsets, and ethernet ports.

- Events and jobs

  View event logs, system alerts, jobs, and audit logs.

- Advanced data protection

  Protect storage VMs, LUNs, and consistency groups.

- Host management

  Set up SAN initiator groups and NFS clients.

Supported configurations

Advanced management through System Manager is supported with Cloud Volumes ONTAP 9.10.0 and later in standard cloud regions.

System Manager integration is not supported in GovCloud regions or in regions that have no outbound internet access.

Limitations

A few features that appear in the System Manager interface are not supported with Cloud Volumes ONTAP:

- Cloud Tiering

  The Cloud Tiering service is not supported with Cloud Volumes ONTAP. Tiering data to object storage must be set up directly from Cloud Manager's Standard View when creating volumes.

- Tiers

  Aggregate management (including local tiers and cloud tiers) is not supported from System Manager. You must manage aggregates directly from Cloud Manager's Standard View.

- Firmware upgrades

  Automatic firmware updates from the **Cluster > Settings** page is not supported with Cloud Volumes ONTAP.

In addition, role-based access control from System Manager is not supported.

How to get started

Open a Cloud Volumes ONTAP working environment and click the Advanced View option.

Steps

1. On the Canvas page, double-click the name of a Cloud Volumes ONTAP system.
2. In the top-right, click **Switch to Advanced View**.
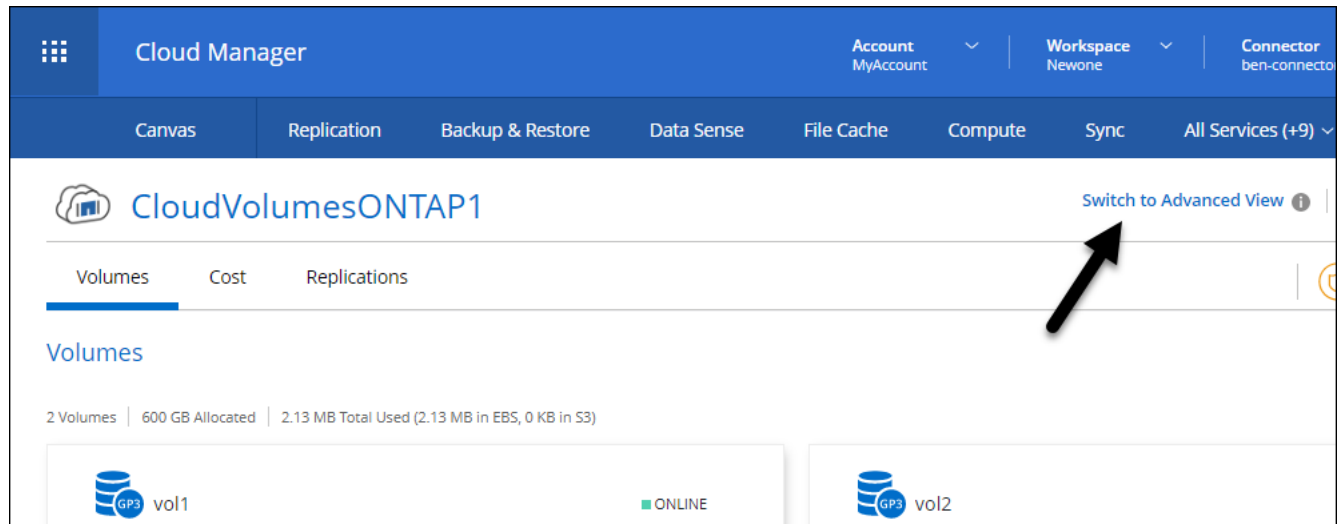
3. If the confirmation message appears, read through it and click **Close**.
4. Use System Manager to manage Cloud Volumes ONTAP.
5. If needed, click **Switch to Standard View** to return to standard management through Cloud Manager.
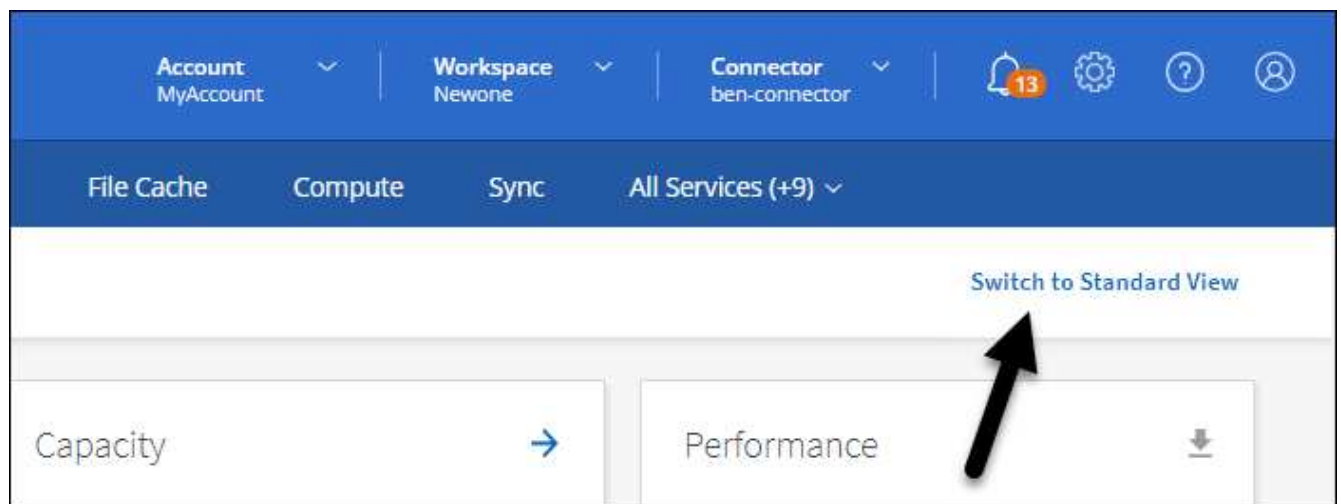
Help with using System Manager

If you need help using System Manager with Cloud Volumes ONTAP, you can refer to ONTAP documentation for step-by-step instructions. Here are a few links that might help:

- Volume and LUN management
- Network management
- Data protection

Administer Cloud Volumes ONTAP from the CLI

The Cloud Volumes ONTAP CLI enables you to run all administrative commands and is a

good choice for advanced tasks or if you are more comfortable using the CLI. You can connect to the CLI using Secure Shell (SSH).

Before you begin

The host from which you use SSH to connect to Cloud Volumes ONTAP must have a network connection to Cloud Volumes ONTAP. For example, you might need to SSH from a jump host that's in your cloud provider network.

> (i) When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

Steps

1. In Cloud Manager, identify the IP address of the cluster management interface:

   a. On the Canvas page, select the Cloud Volumes ONTAP system.

   b. Copy the cluster management IP address that appears in the right pane.

2. Use SSH to connect to the cluster management interface IP address using the admin account.

   Example

   The following image shows an example using PuTTY:

3. At the login prompt, enter the password for the admin account.

   Example

   ```
   Password:  ********
   COT2::>
   ```

System health and events

Verify AutoSupport setup

AutoSupport proactively monitors the health of your system and sends messages to NetApp technical support. By default, AutoSupport is enabled on each node to send messages to technical support using the HTTPS transport protocol. It's best to verify that AutoSupport can send these messages.

The only required configuration step is to ensure that Cloud Volumes ONTAP has outbound internet

connectivity. For details, refer to the networking requirements for your cloud provider.

- AWS networking requirements

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

Configure EMS

The Event Management System (EMS) collects and displays information about events that occur on ONTAP systems. To receive event notifications, you can set event destinations (email addresses, SNMP trap hosts, or syslog servers) and event routes for a particular event severity.

You can configure EMS using the CLI. For instructions, refer to ONTAP docs: EMS configuration overview.

Concepts

Cloud Volumes ONTAP licensing

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

Licensing overview

The following licensing options are available for new customers.

Capacity-based licensing

Pay for multiple Cloud Volumes ONTAP systems in your NetApp account by provisioned capacity. Includes the ability to purchase add-on cloud data services.

Keystone Flex Subscription

A pay-as-you-grow subscription-based service that delivers a seamless hybrid cloud experience for HA pairs.

The previous by-node licensing model remains available for existing customers who have already purchased a license or who have an active marketplace subscription.

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

Capacity-based licensing

Capacity-based licensing packages enable 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. The capacity is 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 several licensing packages based on your business needs.

Packages

The following capacity-based packages are available for Cloud Volumes ONTAP.

Freemium

Provides all Cloud Volumes ONTAP features free of charge from NetApp (cloud provider charges still apply).

- No license or contract is needed.
- Support from NetApp 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, in any cloud provider.

- If the provisioned capacity for a Cloud Volumes ONTAP system exceeds 500 GiB, Cloud Manager converts the system to the Essentials package.

  As soon as a system is converted to the Essentials package, the minimum charge applies.

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

Essentials

Pay by capacity for Cloud Volumes ONTAP in a number of different configurations.

- Choose your Cloud Volumes ONTAP configuration:
    ◦ A single node or HA system
    ◦ File and block storage or secondary data for disaster recovery (DR)
- Add on any of NetApp's cloud data services at extra cost

Professional

Pay by capacity for any type of Cloud Volumes ONTAP configuration with unlimited backups.

- Provides licensing for any Cloud Volumes ONTAP configuration

  Single node or HA with capacity charging for primary and secondary volumes at the same rate

- Includes unlimited volume backups using Cloud Backup, but only for Cloud Volumes ONTAP systems deployed with the Professional package
- Add on any of NetApp's cloud data services at extra cost

Consumption models

Capacity-based licensing packages are available with the following consumption models:

- **BYOL**: A license purchased from NetApp that can be used to deploy Cloud Volumes ONTAP in any cloud provider.
- **PAYGO**: An hourly subscription from your cloud provider's marketplace.
- **Annual**: An annual contract from your cloud provider's marketplace.

Note the following:

- If you purchase a license from NetApp (BYOL), you also need to subscribe to the PAYGO offering from your cloud provider's marketplace.

  Your license is always charged first, but you'll be charged from the hourly rate in the marketplace in these cases:

    ◦ If you exceed your licensed capacity
    ◦ If the term of your license expires
- If you have an annual contract from a marketplace, *all* Cloud Volumes ONTAP systems that you deploy are charged against that contract. You can't mix and match an annual marketplace contract with BYOL.

Changing packages

After deployment, you can change the package for a Cloud Volumes ONTAP system that uses capacity-based licensing. For example, if you deployed a Cloud Volumes ONTAP system with the Essentials package, you can change it to the Professional package if your business needs changed.

Learn how to change charging methods.

Pricing

For details about pricing, go to NetApp Cloud Central.

Free trials

A 30-day free trial is available from the pay-as-you-go subscription in your cloud provider's marketplace. The free trial includes Cloud Volumes ONTAP and Cloud Backup. The trial starts when you subscribe to the offering in the marketplace.

There are no instance or capacity limitations. You can deploy as many Cloud Volumes ONTAP systems as you'd like and allocate as much capacity as needed, free of charge for 30 days. The free trial automatically converts to a paid hourly subscription after 30 days.

There are no hourly software license charges for Cloud Volumes ONTAP, but infrastructure charges from your cloud provider still apply.

> You will receive a notification in Cloud Manager when the free trial starts, when there are 7 days left, and when there is 1 day remaining. For example:
>
>
>
> (i) Your Cloud Manager free trial is almost over (7 days left)
>
> 23 minutes ago | Digital Wallet

Supported configurations

Capacity-based licensing packages are available with Cloud Volumes ONTAP 9.7 and later.

Capacity limit

With this licensing model, each individual Cloud Volumes ONTAP system supports up to 2 PiB of capacity through disks and tiering to object storage.

There is no maximum capacity limitation when it comes to the license itself.

Max number of systems

With capacity-based licensing, the maximum number of Cloud Volumes ONTAP systems is limited to 20 per NetApp account. A *system* is a Cloud Volumes ONTAP HA pair, a Cloud Volumes ONTAP single node system, or any additional storage VMs that you create. The default storage VM does not count against the limit. This limit applies to all licensing models.

For example, let's say you have three working environments:

- A single node Cloud Volumes ONTAP system with one storage VM (this is the default storage VM that's created when you deploy Cloud Volumes ONTAP)

  This working environment counts as one system.

- A single node Cloud Volumes ONTAP system with two storage VMs (the default storage VM, plus one additional storage VM that you created)

  This working environment counts as two systems: one for the single node system and one for the additional storage VM.

- A Cloud Volumes ONTAP HA pair with three storage VMs (the default storage VM, plus two additional storage VMs that you created)

  This working environment counts as three systems: one for the HA pair and two for the additional storage VMs.

That's six systems in total. You would then have room for an additional 14 systems in your account.

If you have a large deployment that requires more then 20 systems, contact your account rep or sales team.

Learn more about NetApp accounts.

Notes about charging

The following details can help you understand how charging works with capacity-based licensing.

Minimum charge

There is a 4 TiB minimum charge for each data-serving storage VM that has least one primary (read-write) volume. If the sum of the primary volumes is less than 4 TiB, then Cloud Manager applies the 4 TiB minimum charge to that storage VM.

If you haven't provisioned any volumes yet, then the minimum charge doesn't apply.

The 4 TiB minimum capacity charge doesn't apply to storage VMs that contain secondary (data protection) volumes only. For example, if you have a storage VM with 1 TiB of secondary data, then you're charged just for that 1 TiB of data.

Overages

If you exceed your BYOL capacity or if your license expires, you'll be charged for overages at the hourly rate based on your marketplace subscription.

Essentials package

With the Essentials package, you're billed by the deployment type (HA or single node) and the volume type (primary or secondary). For example, *Essentials HA* has different pricing than *Essentials Secondary HA*.

If you purchased an Essentials license from NetApp (BYOL) and you exceed the licensed capacity for that deployment and volume type, the Digital Wallet charges overages against a higher priced Essentials license (if you have one). This happens because we first use the available capacity that you've already purchased as prepaid capacity before charging against the marketplace. Charging to the marketplace would add costs to your monthly bill.

Here's an example. Let's say you have the following licenses for the Essentials package:

- A 500 TiB *Essentials Secondary HA* license that has 500 TiB of committed capacity
- A 500 TiB *Essentials Single Node* license that only has 100 TiB of committed capacity

Another 50 TiB is provisioned on an HA pair with secondary volumes. Instead of charging that 50 TiB to PAYGO, the Digital Wallet charges the 50 TiB overage against the *Essentials Single Node* license. That license is priced higher than *Essentials Secondary HA*, but it's cheaper than the PAYGO rate.

In the Digital Wallet, that 50 TiB will be shown as charged against the *Essentials Single Node* license.

Storage VMs

- There are no extra licensing costs for additional data-serving storage VMs (SVMs), but there is a 4 TiB minimum capacity charge per data-serving SVM.
- Disaster recovery SVMs are charged according to the provisioned capacity.

HA pairs

For HA pairs, you're only charged for the provisioned capacity on a node. You aren't charged for data that is synchronously mirrored to the partner node.

FlexClone and FlexCache volumes

- You won't be charged for the capacity used by FlexClone volumes.
- Source and destination FlexCache volumes are considered primary data and charged according to the provisioned space.

How to get started

Learn how to get started with capacity-based licensing:

- Set up licensing for Cloud Volumes ONTAP in AWS

Keystone Flex Subscription

A pay-as-you-grow subscription-based service that delivers a seamless hybrid cloud experience for those preferring OpEx consumption models to upfront CapEx or leasing.

Charging is based on the size of your committed capacity for one or more Cloud Volumes ONTAP HA pairs in your Keystone Flex Subscription.

The provisioned capacity for each volume is aggregated and compared to the committed capacity on your Keystone Flex Subscription periodically, and any overages are charged as burst on your Keystone Flex Subscription.

Learn more about Keystone Flex Subscriptions.

Supported configurations

Keystone Flex Subscriptions are supported with HA pairs. This licensing option isn't supported with single node systems at this time.

Capacity limit

Each individual Cloud Volumes ONTAP system supports up to 2 PiB of capacity through disks and tiering to object storage.

How to get started

Learn how to get started with a Keystone Flex Subscription:

- Set up licensing for Cloud Volumes ONTAP in AWS

Node-based licensing

Node-based licensing is the previous generation licensing model that enabled you to license Cloud Volumes ONTAP by node. This licensing model is not available for new customers and no free trials are available. By-node charging has been replaced with the by-capacity charging methods described above.

Node-based licensing is still available for existing customers:

- If you have an active license, BYOL is available for license renewals only.
- If you have an active marketplace subscription, charging is still available through that subscription.

License conversions

Converting an existing Cloud Volumes ONTAP system to another licensing method isn't supported. The three current licensing methods are capacity-based licensing, Keystone Flex Subscriptions, and node-based licensing. For example, you can't convert a system from node-based licensing to capacity-based licensing (and vice versa).

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

Note that converting a system from PAYGO by-node licensing to BYOL by-node licensing (and vice versa) isn't supported. You need to deploy a new system and then replicate data to that system. Learn how to change between PAYGO and BYOL.

Storage

Client protocols

Cloud Volumes ONTAP supports the iSCSI, NFS, SMB, and S3 client protocols.

iSCSI

iSCSI is a block protocol that can run on standard Ethernet networks. Most client operating systems offer a software initiator that runs over a standard Ethernet port.

NFS

NFS is the traditional file access protocol for UNIX and LINUX systems. Clients can access files in ONTAP volumes using the NFSv3, NFSv4, and NFSv4.1 protocols. You can control file access using UNIX-style permissions, NTFS-style permissions, or a mix of both.

Clients can access the same files using both NFS and SMB protocols.

SMB

SMB is the traditional file access protocol for Windows systems. Clients can access files in ONTAP volumes using the SMB 2.0, SMB 2.1, SMB 3.0, and SMB 3.1.1 protocols. Just like with NFS, a mix of permission styles are supported.

S3

Cloud Volumes ONTAP supports S3 as an option for scale-out storage in the following cloud providers:

- AWS

S3 protocol support enables you to configure S3 client access to objects contained in a bucket in an SVM.

Learn how to configure and manage S3 object storage services in ONTAP.

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. But if you have a configuration that supports the Amazon EBS Elastic Volumes feature, then an aggregate can contain up to 8 disks. Learn more about support for Elastic Volumes.

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

RAID type

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

Hot spares

RAID0 doesn't support the use of hot spares for redundancy.

Creating unused disks (hot spares) attached to a Cloud Volumes ONTAP instance is an unnecessary expense and may prevent provisioning additional space as needed. Therefore, it's not recommended.

Elastic Volumes in AWS

Support for the Amazon EBS Elastic Volumes feature with a Cloud Volumes ONTAP aggregate provides better performance and additional capacity, while enabling Cloud Manager to automatically increase the underlying disk capacity as needed.

Benefits

- Dynamic disk growth

  Cloud Manager can dynamically increase the size of disks while Cloud Volumes ONTAP is running and while disks are still attached.

- Better performance

  Aggregates that are enabled with Elastic Volumes can have up to eight disks that are equally utilized across two RAID groups. This configuration provides more throughput and consistent performance.

- Larger aggregates

  Support for eight disks provides a maximum aggregate capacity of 128 TiB. These limits are higher than the six disk limit and 96 TiB limit for aggregates that aren't enabled with the Elastic Volumes feature.

  Note that total system capacity limits remain the same.

Learn more about Elastic Volumes from AWS

Supported configurations

The Amazon EBS Elastic Volumes feature is supported with specific Cloud Volumes ONTAP versions and

specific EBS disk types.

Cloud Volumes ONTAP version

The Elastic Volumes feature is supported with *new* Cloud Volumes ONTAP systems created from version 9.11.0 or later. The feature is *not* supported with existing Cloud Volumes ONTAP systems that were deployed prior to 9.11.0.

For example, the Elastic Volumes feature is not supported if you created a Cloud Volumes ONTAP 9.9.0 system and then later upgraded that system to version 9.11.0. It must be a new system deployed using version 9.11.0 or later.

EBS disk types

The Elastic Volumes feature is automatically enabled at the aggregate level when using General Purpose SSDs (gp3) or Provisioned IOPS SSDs (io1). The Elastic Volumes feature is not supported with aggregates that use any other disk type.

Required AWS permissions

Starting with the 3.9.19 release, the Connector requires the following permissions to enable and manage the Elastic Volumes feature on a Cloud Volumes ONTAP aggregate:

- ec2:DescribeVolumesModifications
- ec2:ModifyVolume

These permissions are included in the policies provided by NetApp

How support for Elastic Volumes works

An aggregate that has the Elastic Volumes feature enabled is comprised of one or two RAID groups. Each RAID group has four identical disks that have the same capacity. Here's an example of a 10 TiB aggregate that has four disks that are 2.5 TiB each:

When Cloud Manager creates an aggregate, it starts with one RAID group. If additional capacity is needed, Cloud Manager grows the aggregate by increasing the capacity of all disks in the RAID group by the same amount. The capacity increase is either a minimum of 256 GiB or 10% of the aggregate's size.

For example, if you have a 1 TiB aggregate, each disk is 250 GiB. 10% of the aggregate's capacity is 100 GiB. That's lower than 256 GiB, so the size of the aggregate is increased by the 256 GiB minimum (or 64 GiB for each disk).

Cloud Manager increases the size of the disks while the Cloud Volumes ONTAP system is running and while the disks are still attached. The change is non-disruptive.

If an aggregate reaches 64 TiB (or 16 TiB on each disk), Cloud Manager creates a second RAID group for additional capacity. This second RAID group works just like the first one: it has four disks that have the exact same capacity and it can grow up to 64 TiB. That means an aggregate can have a maximum capacity of 128 TiB.

Here's an example of an aggregate with two RAID groups. The capacity limit has been reached on the first RAID group, while the disks in the second RAID group have plenty of free space.

What happens when you create a volume

If you create a volume that uses gp3 or io1 disks, Cloud Manager creates the volume on an aggregate as follows:

- If there is an existing gp3 or io1 aggregate that has Elastic Volumes enabled, Cloud Manager creates the volume on that aggregate.

- If there are multiple gp3 or io1 aggregates that have Elastic Volumes enabled, Cloud Manager creates the volume on the aggregate that requires the least amount of resources.

- If the system only has gp3 or io1 aggregates that aren't enabled for Elastic Volumes, then the volume is created on that aggregate.

> While this scenario is unlikely, it's possible in two cases:
>
> ○ You explicitly disabled the Elastic Volumes feature when creating an aggregate from the API.
>
> ○ You created a new Cloud Volumes ONTAP system from the user interface, in which case the Elastic Volumes feature is disabled on the initial aggregate. Review Limitations below to learn more.

- If no existing aggregates have enough capacity, Cloud Manager creates the aggregate with Elastic Volumes enabled and then creates the volume on that new aggregate.

  The size of the aggregate is based on the requested volume size plus an additional 10% capacity.

Capacity Management Mode

The Capacity Management Mode for a Connector works with Elastic Volumes similar to how it works with other types of aggregates:

- When Automatic mode is enabled (this is the default setting), Cloud Manager automatically increases the size of aggregates if additional capacity is needed.

- If you change the capacity management mode to Manual, Cloud Manager asks for your approval to purchase additional capacity.

Learn more about the Capacity Management Mode.

Limitations

Increasing the size of an aggregate can take up to 6 hours. During that time, Cloud Manager can't request any additional capacity for that aggregate.

How to work with Elastic Volumes

You can work with Elastic Volumes in Cloud Manager as follows:

- Create a new system that has Elastic Volumes enabled on the initial aggregate when using gp3 or io1 disks

  Learn how to create Cloud Volumes ONTAP system

- Create a new volume on an aggregate that has Elastic Volumes enabled

  If you create a volume that uses gp3 or io1 disks, Cloud Manager automatically creates the volume on an aggregate that has Elastic Volumes enabled. For more details, refer to What happens when you create a volume.

  Learn how to create volumes.

- Create a new aggregate that has Elastic Volumes enabled

Elastic Volumes is automatically enabled on new aggregates that use gp3 or io1 disks, as long as the Cloud Volumes ONTAP system was created from version 9.11.0 or later.

When you create the aggregate, Cloud Manager will prompt you for the aggregate's capacity size. This is different than other configurations where you choose a disk size and number of disks.

The following screenshot shows an example of a new aggregate comprised of gp3 disks.

[Learn how to create aggregates](#).

- Identify aggregates that have Elastic Volumes enabled

When you go to the Advanced Allocation page, you can identify whether the Elastic Volumes feature is enabled on an aggregate. In the following example, aggr2 has Elastic Volumes enabled whereas aggr1 does not.

- Add capacity to an aggregate

While Cloud Manager automatically adds capacity to aggregates as needed, you can manually increase the capacity yourself.

[Learn how to increase aggregate capacity](#).

- Replicate data to an aggregate that has Elastic Volumes enabled

If the destination Cloud Volumes ONTAP system supports Elastic Volumes, a destination volume will be placed on an aggregate that has Elastic Volumes enabled (as long as you choose a gp3 or io1 disk).

Learn how to set up data replication

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.
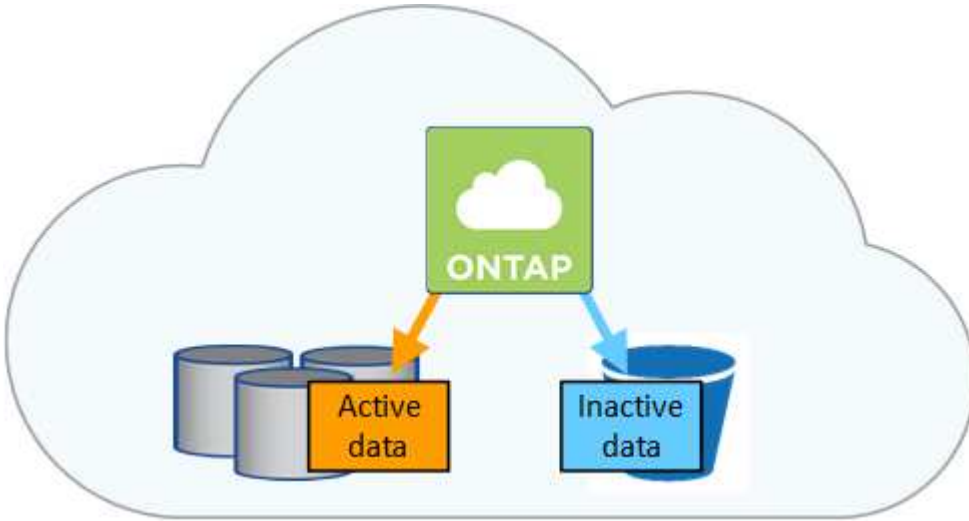
Data tiering is powered by FabricPool technology.

ⓘ | 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.

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.

When Cloud Manager creates the S3 bucket, it uses the following default settings:

- Storage class: Standard
- Default encryption: Disabled

- Block public access: Block all public access

- Object ownership: ACLs enabled

- Bucket versioning: Disabled

- Object lock: Disabled

Storage classes

The default storage class for tiered data in AWS is *Standard*. Standard is ideal for frequently accessed data stored across multiple Availability Zones.

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*, *Standard-Infrequent Access*, or *S3 Glacier Instant Retrieval*. 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 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.

  In the case of an aggregate in AWS that supports Elastic Volumes, Cloud Manager also increases the size of the disks in a RAID group. Learn more about support for Elastic Volumes.

- 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:

Aggregate number	Disk size	Max aggregate capacity
1	500 GiB	3 TiB
4	1 TiB	6 TiB
6	2 TiB	12 TiB

> ℹ️ This behavior does not apply to aggregates that support the Amazon EBS Elastic Volumes feature. Aggregates that have Elastic Volumes enabled are comprised of one or two RAID groups. Each RAID group has four identical disks that have the same capacity. Learn more about support for Elastic Volumes.

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.

This behavior is determined by the *Capacity Management Mode* on a Connector. The Capacity Management Mode affects all Cloud Volumes ONTAP systems managed by that Connector. If you have another Connector, it can be configured differently.

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 reaches the capacity threshold and it has room for more disks, 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.

  In the case of an aggregate in AWS that supports Elastic Volumes, Cloud Manager also increases the size of the disks in a RAID group. Learn more about support for Elastic Volumes.

- If an aggregate reaches the capacity threshold and it can't support any additional disks, 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 the cloud provder 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.

Learn more

Learn how to modify the capacity management mode.

Write speed

Cloud Manager enables you to choose normal or high write speed for most Cloud Volumes ONTAP configurations. 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.

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.

High write speed with an HA pair in AWS

If you plan to enable high write speed on an HA pair in AWS, you should understand the difference in protection levels between a multiple Availability Zone (AZ) deployment and a single AZ deployment. Deploying an HA pair across multiple AZs provides more resiliency and can help to mitigate the chance of data loss.

Learn more about HA pairs in AWS.

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](#).

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 data loss occurs due to high write speed, the Event Management System (EMS) reports the following two events:

- Cloud Volumes ONTAP 9.11.0 or later

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

- Cloud Volumes ONTAP 9.8 to 9.10.1

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

When this happens, Cloud Volumes ONTAP should be able to boot up and continue to serve data without user intervention.

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 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 configurations

Flash Cache is supported with specific Cloud Volumes ONTAP configurations. View supported configurations in the Cloud Volumes ONTAP Release Notes

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. Cloud WORM storage is powered by SnapLock technology, which means WORM files are protected at the file level.

How WORM storage works

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.

Charging

Charging for WORM storage is hourly, according to the total provisioned capacity of WORM volumes.

Learn about pricing for WORM storage.

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.

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.

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.

HA components

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.

Mediator

Here are some key details about the mediator instance in AWS:

Instance type
 t2-micro

Disks
 One EBS magnetic disk that is approximately 8 GiB.

Operating system
 Debian 11

> ⓘ   For Cloud Volumes ONTAP 9.10.0 and earlier, Debian 10 was installed on the mediator.

Upgrades
 When you upgrade Cloud Volumes ONTAP, Cloud Manager also updates the mediator instance as needed.

Access to the instance

When you create a Cloud Volumes ONTAP HA pair from Cloud Manager, you're prompted to provide a key pair for the mediator instance. You can use that key pair for SSH access using the `admin` user.

Third-party agents

Third-party agents or VM extensions are not supported on the mediator instance.

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**.

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.

> ℹ️ 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.

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

Performance expectations

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

- For HA configurations that serve data from only one node, read performance is comparable to the read performance of a single-node configuration, whereas write performance is lower.

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

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

Client access to storage

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

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

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

Volumes

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

vol1		**ⓘ Info** **✏ Edit** **🗑 Delete**	✕
🗐 Clone		↗ Mount Command	
↺ Restore from Snapshot copy		⊟ Change Tier	

Actions unavailable during takeover

When a node in an HA pair isn't available, the other node serves data for its partner to provide continued data service. This is called *storage takeover*. Several actions are unavailable until in storage giveback is complete.

> **💡** When a node in an HA pair is unavailable, the state of the working environment in Cloud Manager is *Degraded*.

The following actions are unavailable from Cloud Manager during storage takeover:

- Support registration
- License changes
- Instance or VM type changes
- Write speed changes
- CIFS setup
- Changing the location of configuration backups
- Setting the cluster password
- Managing disks and aggregates (advanced allocation)

These actions are available again after storage giveback completes and the state of the working environment changes back to normal.

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

You can use NetApp encryption solutions with native encryption from your cloud provider, which encrypts 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 NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE). NVE and NAE are software-based solutions that enable (FIPS) 140-2–compliant data-at-rest encryption of volumes. Both NVE and NAE use AES 256-bit encryption.

- 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 are supported with an external key manager.

New aggregates 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, refer to 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.

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.

Performance technical reports

- Cloud Volumes ONTAP for AWS

CPU performance

Cloud Volumes ONTAP nodes show as highly utilized (over 90%) from your cloud provider's monitoring tools. This is because ONTAP reserves all vCPUs presented to the virtual machine so that they are available when needed.

Learn how to monitor Cloud Volumes ONTAP performance, or check out this NetApp knowledgebase article about how to monitor ONTAP CPU utilization using the CLI

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.

> 💡 A node-based license is the previous generation BYOL for Cloud Volumes ONTAP. A node-based license is available for license renewals only.

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 PiB.

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

> ℹ️ 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

.

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.

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.

Default setup

- 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
  - Multi-tenant Encryption Key Management (MTEKM), starting with Cloud Volumes ONTAP 9.11.1
  - NetApp Volume Encryption (only for BYOL or registered PAYGO systems)
  - NFS
  - ONTAP S3

    Starting with Cloud Volumes ONTAP 9.11.0 in AWS

  - SnapMirror
  - SnapRestore
  - SnapVault

- Several network interfaces are created by default:
  - A cluster management LIF
  - An intercluster LIF
  - An SVM management LIF on single node systems in AWS
  - A node management LIF
  - An iSCSI data LIF
  - A CIFS and NFS data LIF

    > LIF failover is disabled by default for Cloud Volumes ONTAP due to cloud provider 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 ℹ️ The Account Admin can modify this value from the Settings page.
Security style	NTFS for CIFS volumes UNIX for NFS volumes
Space guarantee style	none
UNIX permissions (NFS only)	777

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

Internal disks for system data

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

AWS

- Three disks per node for boot, root, and core data:
    - 45 GiB io1 disk for boot data
    - 140 GiB gp3 disk for root data
    - 540 GiB gp2 disk for core data
- 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
- 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.

💡 In AWS, NVRAM is on the boot disk.

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.

Knowledge and support

Register for support

Before you can open a support case with NetApp technical support, you need to add a NetApp Support Site account to Cloud Manager and then register for support.

Add an NSS account

The Support Dashboard enables you to add and manage all of your NetApp Support Site accounts from a single location.

Steps

1. If you don't have a NetApp Support Site account yet, register for one.

2. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

3. Click **NSS Management > Add NSS Account**.

4. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

5. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

   This action enables Cloud Manager to use your NSS account.

   Note the account must be a customer-level account (not a guest or temp account).

Register your account for support

Support registration is available from Cloud Manager in the Support Dashboard.

Steps

1. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

2. In the **Resources** tab, click **Register for Support**.
3. Select the NSS credentials that you want to register and then click **Register**.

Get help

NetApp provides support for Cloud Manager and its cloud services in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Self support

These options are available for free, 24 hours a day, 7 days a week:

- Knowledge base

  Search through the Cloud Manager knowledge base to find helpful articles to troubleshoot issues.

- Communities

  Join the Cloud Manager community to follow ongoing discussions or create new ones.

- Documentation

  The Cloud Manager documentation that you're currently viewing.

- Feedback email

  We value your input. Submit feedback to help us improve Cloud Manager.

NetApp support

In addition to the self-support options above, you can work with a NetApp Support Engineer to resolve any issues after you activate support.

Steps

1. In Cloud Manager, click **Help > Support**.

2. Choose one of the available options under Technical Support:

   a. Click **Call Us** to find phone numbers for NetApp technical support.

   b. Click **Open an Issue**, select one the options, and then click **Send**.

   A NetApp representative will review your case and get back to you soon.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

Notice for Cloud Manager 3.9