

NetApp *Cloud Docs*

NetApp Docs

2020

Table of Contents

1. Cloud Manager and Cloud Volumes ONTAP documentation	1
1.1. Discover what's new	1
1.2. Get started	1
1.3. Automate with APIs	1
1.4. Learn about Cloud Manager and Cloud Volumes ONTAP	1
1.5. Connect with peers, get help, and find more information	1
2. Release notes	2
2.1. Cloud Manager	2
3. Concepts	8
3.1. Cloud Manager and Cloud Volumes ONTAP overview	8
3.2. NetApp Cloud Central	9
3.3. Storage	10
3.4. Storage management	14
3.5. High-availability pairs	20
3.6. Security	25
3.7. WORM storage	25
3.8. Licensing	26
3.9. Performance	27
3.10. Cloud Storage Automation	27
4. Getting started	30
4.1. Deployment overview	30
4.2. Getting started with Cloud Volumes ONTAP in AWS	31
4.3. Getting started with Cloud Volumes ONTAP in Azure	32
4.4. Setting up Cloud Manager	33
4.5. Detailed networking requirements	39
4.6. Additional deployment options	50
4.7. Additional ways to provide permissions	58
5. Deploying Cloud Volumes ONTAP	65
5.1. Before you create Cloud Volumes ONTAP systems	65
5.2. Logging in to Cloud Manager	65
5.3. Planning your Cloud Volumes ONTAP configuration	66
5.4. Launching Cloud Volumes ONTAP in AWS	71
5.5. Launching Cloud Volumes ONTAP in Azure	80
5.6. Registering pay-as-you-go systems	84
5.7. Setting up Cloud Volumes ONTAP	85
6. Provisioning storage	88
6.1. Provisioning storage	88
6.2. Tiering cold data to low-cost object storage	92

6.3. Managing existing storage	94
6.4. Provisioning NFS volumes from the Volume View	100
7. Managing data across a hybrid cloud	106
7.1. Discovering and managing ONTAP clusters	106
7.2. Replicating data to and from the cloud	108
7.3. Syncing data to AWS S3	115
8. Administering Cloud Volumes ONTAP	117
8.1. Connecting to Cloud Volumes ONTAP	117
8.2. Updating Cloud Volumes ONTAP software	118
8.3. Modifying Cloud Volumes ONTAP systems	122
8.4. Managing the state of Cloud Volumes ONTAP	126
8.5. Monitoring AWS storage and compute costs	127
8.6. Adding existing Cloud Volumes ONTAP systems to Cloud Manager	128
8.7. Deleting a Cloud Volumes ONTAP working environment	128
9. Administering Cloud Manager	130
9.1. Updating Cloud Manager	130
9.2. Backing up and restoring Cloud Manager	131
9.3. Removing Cloud Volumes ONTAP working environments	132
9.4. Editing user accounts	133
9.5. Configuring Cloud Manager to use a proxy server	133
9.6. Managing encryption settings for Cloud Volumes ONTAP	134
9.7. Renewing the Cloud Manager HTTPS certificate	136
9.8. Uninstalling Cloud Manager	136
10. Reference	138
10.1. Frequently asked questions: Integrating Cloud Manager with NetApp Cloud Central	138
10.2. Supported regions	139
10.3. Security group rules for AWS	141
10.4. Security group rules for Azure	148
10.5. Cloud Manager REST APIs	153
10.6. AWS and Azure permissions for Cloud Manager	154
10.7. Default configurations	159
10.8. User roles	161
10.9. Where to get help and find more information	162
11. Earlier versions of Cloud Manager documentation	164

1. Cloud Manager and Cloud Volumes ONTAP documentation

OnCommand Cloud Manager enables you to deploy and manage NetApp Cloud Volumes ONTAP (formerly ONTAP Cloud), which is a data management solution that provides protection, visibility, and control for your cloud-based workloads.

1.1. Discover what's new

- [What's new in Cloud Manager](#)
- [What's new in Cloud Volumes ONTAP](#)

1.2. Get started

- [Get started in AWS](#)
- [Get started in Azure](#)
- [Find supported configurations for Cloud Volumes ONTAP](#)
- [Review detailed networking requirements for Cloud Manager](#)
- [Review detailed networking requirements for Cloud Volumes ONTAP for AWS](#)
- [Review detailed networking requirements for Cloud Volumes ONTAP for Azure](#)
- [Plan your Cloud Volumes ONTAP configuration](#)

1.3. Automate with APIs

[OnCommand Cloud Manager API Developer Guide](#)

1.4. Learn about Cloud Manager and Cloud Volumes ONTAP

▶ <https://www.youtube.com/watch?v=9I5QToO6ZpU> (YouTube video)

[Watch additional videos](#)

1.5. Connect with peers, get help, and find more information

- [NetApp Community: Hybrid Cloud](#)
- [NetApp Cloud Volumes ONTAP Support](#)
- [Where to get help and find more information](#)

2. Release notes

2.1. Cloud Manager

2.1.1. What's new in Cloud Manager 3.5

OnCommand Cloud Manager typically introduces a new release every month to bring you new features, enhancements, and bug fixes.

Cloud Manager 3.5.3 (2 Sept 2018)

Cloud Manager 3.5.3 includes a few enhancements.

- [Creation of SVM management LIF for HA systems in multiple AZs](#)
- [Ability to break SMB/CIFS locks](#)

Creation of SVM management LIF for HA systems in multiple AZs

When deploying Cloud Volumes ONTAP HA systems in multiple Availability Zones, you can now specify the floating IP address for an SVM management network interface (LIF). The SVM management LIF enables you to use SnapCenter or SnapDrive for Windows with the HA system.

[Shows the Floating IPs page in the Create a New Working Environment wizard. The fourth text box enables you to specify a floating IP address for the SVM management LIF.]

Ability to break SMB/CIFS locks

In previous releases, upgrading or modifying the instance type and license type for a Cloud Volumes ONTAP HA system could fail if locks were present on SMB/CIFS files. Starting in this release, Cloud Manager can detect and break the locks before it proceeds with the operation. You simply need to confirm when prompted.

Cloud Manager 3.5.2 (1 Aug 2018)

Cloud Manager 3.5.2 includes new features and enhancements.



Changes in this release require a new Azure permission for Cloud Manager. Read the changes below.

- [Support for WORM storage](#)
- [Support for the auto tiering policy with Cloud Volumes ONTAP Standard](#)
- [Cloud Manager deployment in Azure from NetApp Cloud Central](#)
- [Animation added to used capacity charts](#)
- [Locks on Azure disks](#)
- [Tags on AWS CloudFormation stacks](#)

- [Deprecation of Cloud Volumes ONTAP encryption in AWS](#)

Support for WORM storage

You can now activate WORM storage on new Cloud Volumes ONTAP systems. Write once, read many (WORM) storage enables you to retain critical files in unmodified form for regulatory and governance purposes and to protect from malware attacks. WORM files are protected at the file level.

[Learn more about WORM storage.](#)

Support for the auto tiering policy with Cloud Volumes ONTAP Standard

The *auto* volume tiering policy is now supported with the pay-as-you-go Standard license for Cloud Volumes ONTAP. You can select the auto tiering policy when creating, modifying, or replicating a volume. Data tiering enables automated tiering of cold data to low-cost object storage.



Auto is the default policy when creating new volumes for Cloud Volumes ONTAP Standard, Premium, and BYOL.

[Learn more about data tiering.](#)

Cloud Manager deployment in Azure from NetApp Cloud Central

You can now deploy new Cloud Manager systems in Microsoft Azure directly from [NetApp Cloud Central](#). Cloud Central simplifies the deployment experience and provides a single location to view and manage multiple Cloud Manager systems. Providing your Azure credentials is secure and private because they are entered in an Azure pop-up window.

[Learn more about Cloud Central.](#)

Animation added to used capacity charts

An animation now shows you the amount of used capacity when you view volumes or aggregates.

[An animated screenshot that shows an aggregate and its used capacity.]

Locks on Azure disks

Cloud Manager can now add locks to the Azure disks that it allocates to Cloud Volumes ONTAP. The locks help to ensure that the disks are not accidentally deleted. This change requires a new permission so Cloud Manager can add, delete, and query the locks:

```
"Microsoft.Authorization/locks/*"
```

You should add this permission to the custom role that provides Cloud Manager with the required permissions.

Tags on AWS CloudFormation stacks

Cloud Manager now adds user tags to the AWS CloudFormation stacks that it creates. The tags can help to ensure that the stacks are not deleted by automated processes.

Deprecation of Cloud Volumes ONTAP encryption in AWS

Data-at-rest encryption of aggregates using external key managers is no longer supported when launching new Cloud Volumes ONTAP systems in AWS. Existing systems that use this feature are still supported; however, Cloud Volumes ONTAP encryption will be deprecated in the 9.5 release. NetApp will contact you to discuss how to upgrade those systems to the 9.5 release and how to implement a replacement encryption feature.

You can still enable data encryption on new systems by using the AWS Key Management Service (KMS).

Cloud Manager 3.5.1 (2 July 2018)

Cloud Manager 3.5.1 includes new features and enhancements.

- [Support for pay-as-you-go in the AWS GovCloud \(US\) region](#)
- [Tiering levels for cold data](#)
- [Providing Azure permissions using a Managed Service Identity](#)
- [New used capacity charts](#)

Support for pay-as-you-go in the AWS GovCloud (US) region

The pay-as-you-go version of Cloud Volumes ONTAP is now supported in the AWS GovCloud (US) region. This is in addition to supporting Cloud Volumes ONTAP BYOL in the GovCloud (US) region.

You can deploy Cloud Volumes ONTAP in the GovCloud (US) region just like any other region. Go to NetApp Cloud Central and launch Cloud Manager in GovCloud (US). Then launch Cloud Volumes ONTAP PAYGO or BYOL by creating a new working environment in Cloud Manager.

Tiering levels for cold data

After you deploy Cloud Volumes ONTAP, you can change the Amazon S3 storage class or the Azure Blob storage tier in which you want to store cold data. Changing the tiering level can reduce your storage costs, if you do not plan to access the data. The access costs are higher if you do access the data, so you must take that into consideration before you change the tiering level.

The tiering level is system wide—it is not per volume. For details about changing the tiering level, see [Tiering cold data to low-cost object storage](#).

AWS tiering levels

In AWS, Cloud Volumes ONTAP uses **Standard** as the default storage class for data tiering to Amazon S3. You can change the storage class to either **Standard-Infrequent Access** or **One Zone-Infrequent Access**. When you change the tiering level, cold data starts in the **Standard** storage class and moves to the storage class that you selected, if the data is not accessed after 30 days. For details about S3 storage classes, refer to [AWS documentation](#).

[A screenshot that shows the three S3 storage classes.]

Azure tiering levels

In Azure, Cloud Volumes ONTAP uses the Azure **hot** storage tier as the default for data tiering to Blob storage. You can change to the Azure **cool** storage tier. When you change the tiering level, cold data starts in the **hot** storage tier and moves to the **cool** storage tier, if the data is not accessed after 30 days. For details about Azure Blob storage tiers, refer to [Azure documentation](#).

[A screenshot that shows the two Blob storage tiers.]

Providing Azure permissions using a Managed Service Identity

You can now provide Azure permissions to Cloud Manager by using a Managed Service Identity. A Managed Service Identity allows a Cloud Manager virtual machine in Azure to identify itself to Azure Active Directory without providing any credentials. This method is simpler than manually setting up an Azure service principal and providing the credentials to Cloud Manager.

To use a Managed Service Identity with Cloud Manager, follow [instructions for new Cloud Manager virtual machines](#) or [instructions for existing Cloud Manager virtual machines](#).



Managed Service Identities are not supported in the Azure US Gov regions and in the Germany regions. You must [grant Azure permissions to Cloud Manager using a service principal and credentials](#).

For more information about Managed Service Identities, refer to [Azure documentation](#).

New used capacity charts

Cloud Manager now provides a graphical representation of used capacity when viewing volumes and aggregates.

[A screenshot that shows a volume and its used capacity.]

Cloud Manager 3.5 (3 June 2018)

Cloud Manager 3.5 includes new features and enhancements.

- [Support for Cloud Volumes ONTAP 9.4](#)
- [New permissions required for Cloud Volumes ONTAP 9.4](#)
- [Cloud Manager integration with NetApp Cloud Central](#)
- [Support for the m4.large instance type](#)
- [Marketplace image now based on RHEL 7.4](#)

Support for Cloud Volumes ONTAP 9.4

You can now deploy new Cloud Volumes ONTAP 9.4 systems from Cloud Manager and upgrade your existing systems to the 9.4 release. Cloud Manager also provides support for [the new features introduced in Cloud Volumes ONTAP 9.4](#).

New permissions required for Cloud Volumes ONTAP 9.4

Cloud Manager requires new permissions for key features in the Cloud Volumes ONTAP 9.4 release. To ensure that your Cloud Manager systems can deploy and manage Cloud Volumes ONTAP 9.4 systems, you must update your Cloud Manager policy by adding the following permissions:

- For AWS: "ec2:DescribeInstanceAttribute",

Cloud Manager uses this permission to verify that enhanced networking is enabled for supported instance types.

- For Azure: "Microsoft.Network/virtualNetworks/subnets/write",

Cloud Manager uses this permission to enable VNet service endpoints for data tiering.

You can find the entire list of required permissions in [the latest policies provided by NetApp](#).

Cloud Manager integration with NetApp Cloud Central

When upgrading to Cloud Manager 3.5, NetApp will choose specific Cloud Manager systems to integrate with NetApp Cloud Central, if they are not already integrated. During this process, NetApp migrates all local user accounts in your Cloud Manager system to the centralized user authentication available in Cloud Central. After the upgrade is complete, you simply need to log in.

If you have questions, refer to [this FAQ](#).

Support for the m4.large instance type

Cloud Manager is now supported with the m4.large EC2 instance type. m3.large is no longer supported.

For a list of supported Cloud Manager configurations, see [Cloud Manager host requirements](#).

Marketplace image now based on RHEL 7.4

The operating system for the Cloud Manager marketplace image in AWS and Azure is now Red Hat Enterprise Linux 7.4.

2.1.2. Known issues

Known issues identify problems that might prevent you from using this release of the product successfully.

There are no known issues in this release of Cloud Manager.

You can find known issues for Cloud Volumes ONTAP in the [Cloud Volumes ONTAP Release Notes](#) and for ONTAP software in general in the [ONTAP Release Notes](#).

2.1.3. 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.

Active Directory not supported by default with new installations of Cloud Manager

Starting with version 3.4, new installations of Cloud Manager do not support using your organization's Active Directory authentication for user management. If needed, NetApp can help you set up Active Directory with Cloud Manager. Click the chat icon in the lower right of Cloud Manager to get assistance.

Limitations with the AWS GovCloud (US) region

- Cloud Manager must be deployed in the AWS GovCloud (US) region if you want to launch Cloud Volumes ONTAP instances in the AWS GovCloud (US) region.
- When deployed in the AWS GovCloud (US) region, Cloud Manager cannot discover ONTAP clusters in a NetApp Private Storage for Microsoft Azure configuration or a NetApp Private Storage for SoftLayer configuration.

Volume View limitations

- The Volume View is not supported in the AWS GovCloud (US) region, in the AWS Commercial Cloud Services environment, and in Microsoft Azure.
- The Volume View enables you to create NFS volumes only.
- Cloud Manager does not launch Cloud Volumes ONTAP BYOL instances in the Volume View.

Cloud Manager does not verify IP addresses of key managers

When you add a key manager to Cloud Manager, it does not verify the IP address that you entered because Cloud Manager does not communicate with key managers. If the IP address is incorrect, you are notified later when you try to create a Cloud Volumes ONTAP working environment. Be sure to verify key manager IP addresses after you enter them.

Cloud Manager does not set up iSCSI volumes

When you create a volume in Cloud Manager using the Storage System View, you can choose the NFS or CIFS protocol. You must use OnCommand System Manager to create a volume for iSCSI.

Storage Virtual Machine (SVM) limitation

Cloud Volumes ONTAP supports one data-serving SVM and one or more SVMs used for disaster recovery.

Cloud Manager does not provide any setup or orchestration support for SVM disaster recovery. It also does not support storage-related tasks on any additional SVMs. You must use System Manager or the CLI for SVM disaster recovery.

3. Concepts

3.1. Cloud Manager and Cloud Volumes ONTAP overview

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

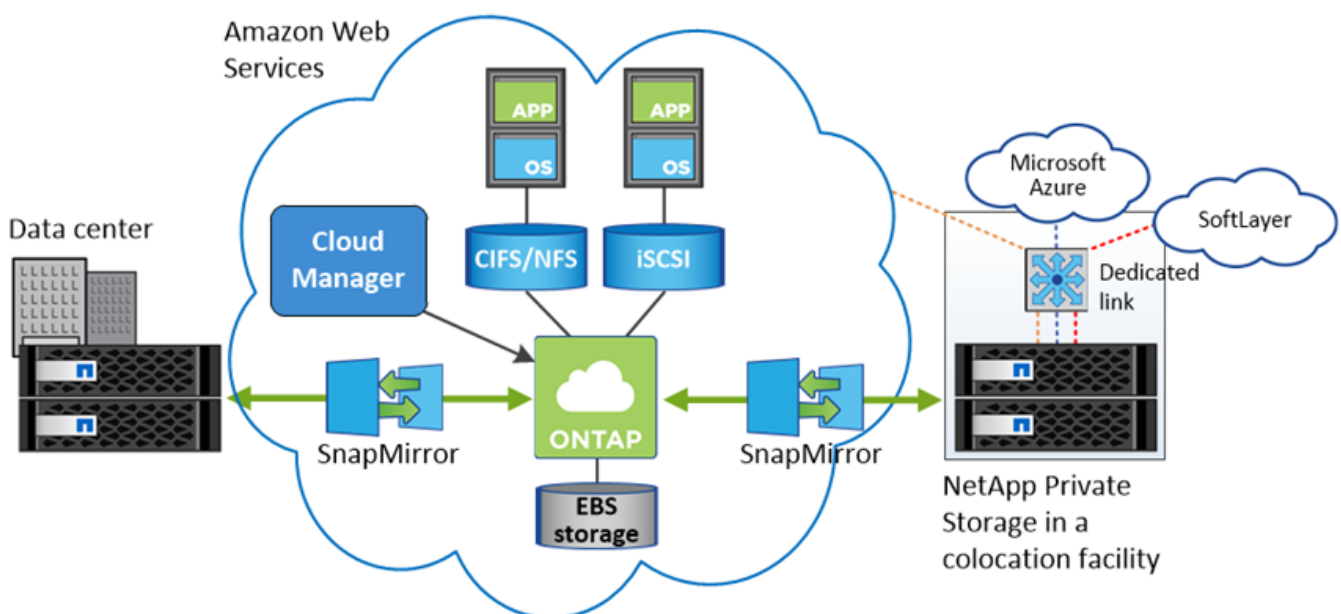
3.1.1. Cloud Manager

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

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

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

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



[Learn more about Cloud Manager](#)

3.1.2. Cloud Volumes ONTAP

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

Cloud Volumes ONTAP extends enterprise storage to the cloud with the following key features:

- **Storage efficiencies**
Leverage built-in data deduplication, data compression, thin provisioning, and cloning to minimize storage costs.
- **High availability**
Ensure enterprise reliability and continuous operations in case of failures in your cloud environment (AWS only).
- **Data replication**
Cloud Volumes ONTAP leverages SnapMirror, NetApp's industry-leading replication technology, to replicate on-premises data to the cloud so it's easy to have secondary copies available for multiple use cases.
- **Data tiering**
Switch between high and low-performance storage pools on-demand without taking applications offline.
- **Application consistency**
Ensure consistency of NetApp Snapshot copies using the NetApp SnapManager tool suite.



Licenses for ONTAP features are included with Cloud Volumes ONTAP.

[View supported Cloud Volumes ONTAP configurations](#)

[Learn more about Cloud Volumes ONTAP](#)

3.2. NetApp Cloud Central

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

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

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

The following video provides an overview of NetApp Cloud Central:

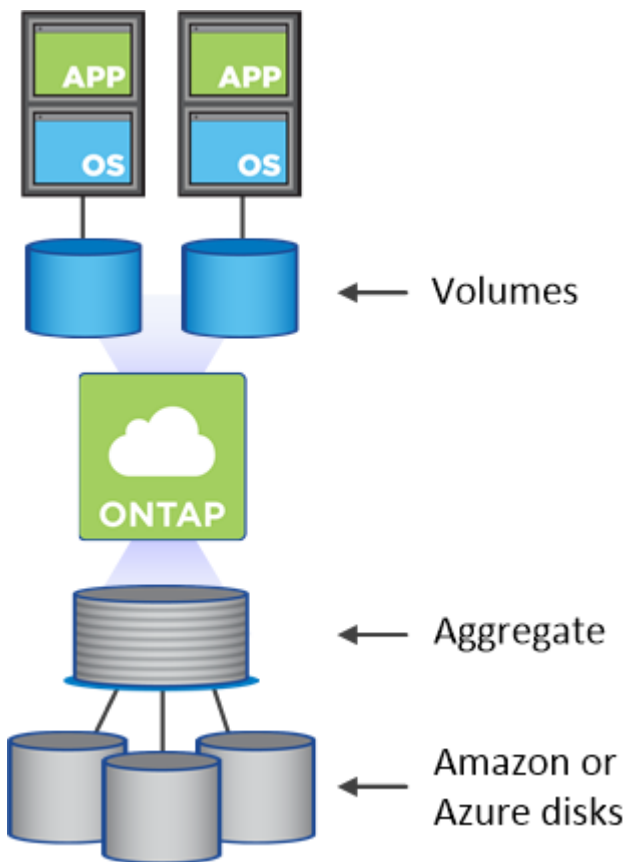
► <https://www.youtube.com/watch?v=xKRsfIfiy-54> (YouTube video)

3.3. Storage

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

3.3.1. How Cloud Volumes ONTAP uses cloud storage

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



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

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

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

- [Choosing an AWS disk type](#)

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



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

3.3.2. Data tiering overview

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

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

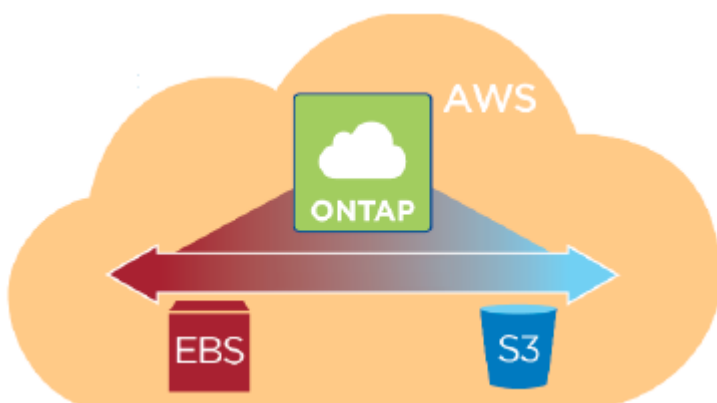


You do not need to install a feature license to enable data tiering.

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

How data tiering works in AWS

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



Performance tier in AWS

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

Capacity tier in AWS

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

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

Standard-Infrequent Access

For infrequently accessed data stored across multiple Availability Zones.

One Zone-Infrequent Access

For infrequently accessed data stored in a single Availability Zone.

The access costs are higher if you do access the data, so you must take that into consideration before you change the tiering level. For more details about S3 storage classes, refer to [AWS documentation](#).

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

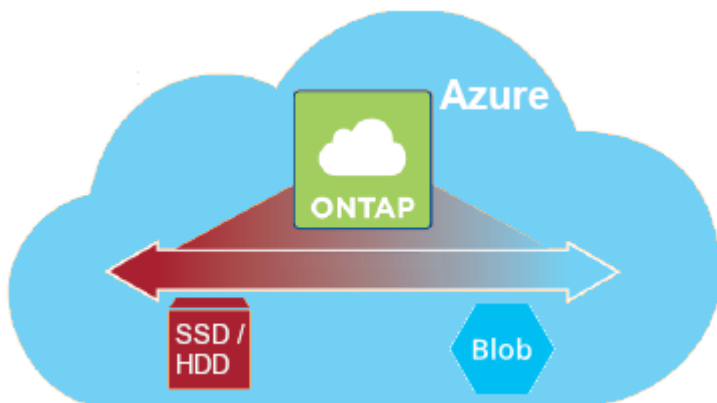
The tiering level is system wide—it is not per volume.



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

How data tiering works in Microsoft Azure

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



Performance tier in Azure

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

Capacity tier in Azure

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

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

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

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

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



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

How data tiering affects capacity limits

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

Volume tiering policies

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

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

Cloud Volumes ONTAP supports the following tiering policies:

Snapshot Only

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

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

Auto

After an aggregate has reached 50% capacity, Cloud Volumes ONTAP tiers cold data blocks in a volume to a capacity tier. The cold data includes not just Snapshot copies but also cold user data

from the active file system. The cooling period is approximately 31 days.

This policy is supported starting with Cloud Volumes ONTAP 9.4.

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

Backup

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

None

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

Setting up data tiering

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

3.4. Storage management

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



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

3.4.1. Storage provisioning

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

Simplified provisioning

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

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

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

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



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

Disk size selection for aggregates in AWS

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

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

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

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

Advanced allocation

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

3.4.2. Capacity management

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

Automatic capacity management

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

The following examples illustrate how this mode works:

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

- If an aggregate with 12 Azure disks reaches the capacity threshold, Cloud Manager automatically moves a volume from that aggregate to an aggregate with available capacity or to a new aggregate.

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

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

Manual capacity management

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

3.4.3. Storage isolation using tenants

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

Working environments

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

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

The following image shows a Cloud Volumes ONTAP working environment:

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

Tenants

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

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

User management of tenants and working environments

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

Cloud Manager Admin

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

Tenant Admin

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

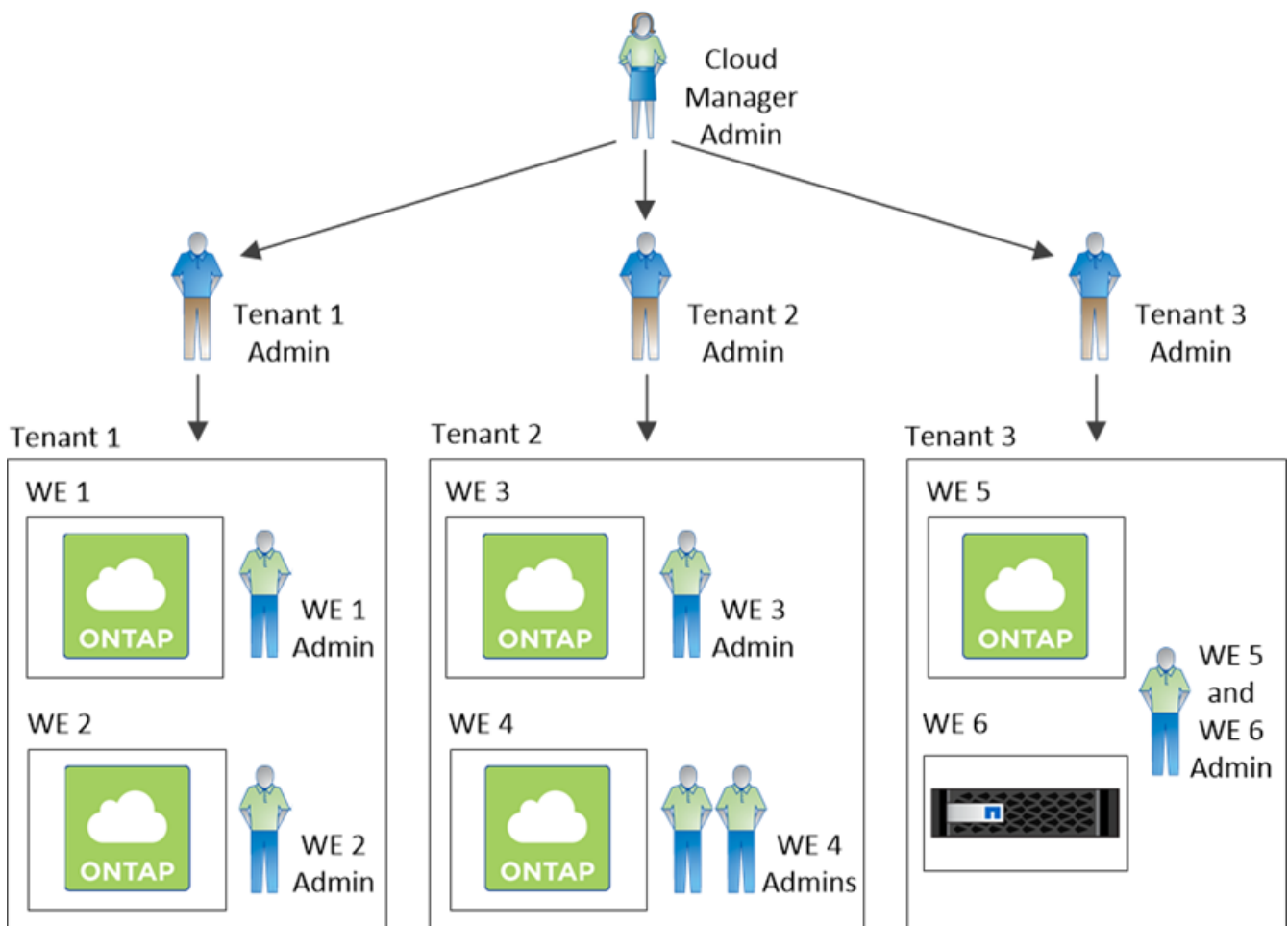
Working Environment Admin

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

Example of how you can create tenants and users

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

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



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

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

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

► https://www.youtube.com/watch?v=_8s16fS_L1Y (YouTube video)

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

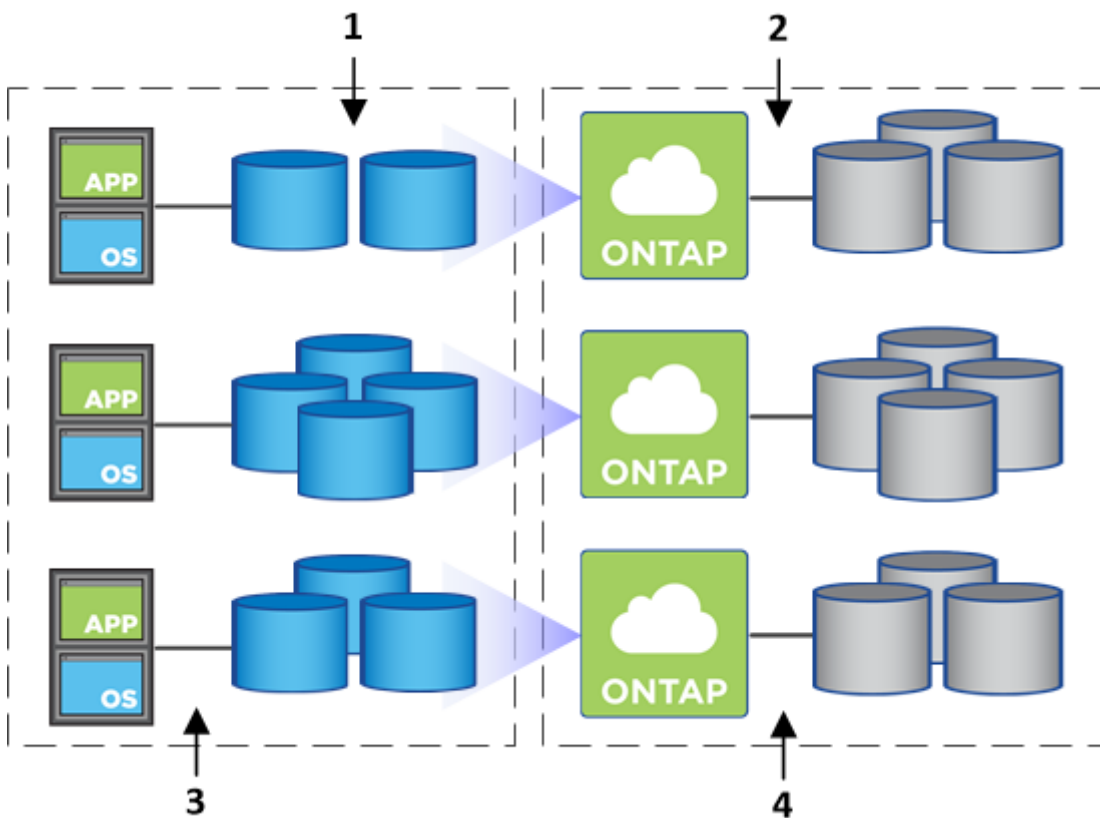
For more information about how Cloud Manager manages license files, refer to [Licensing](#).

3.4.4. Simplified storage management using the Volume View

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

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

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

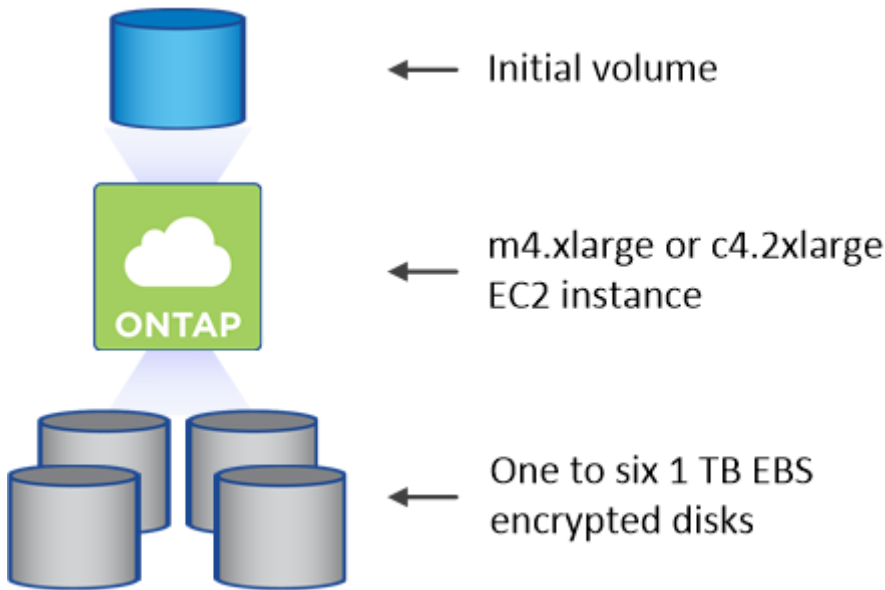


1. You create NFS volumes.
2. Cloud Manager launches Cloud Volumes ONTAP instances in AWS for new volumes or it creates volumes on existing instances. It also purchases physical EBS storage for the volumes.
3. You make the volumes available to your hosts and applications.
4. Cloud Manager makes capacity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

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

Allocation of cloud resources for the initial volume

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



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



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



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

Allocation of cloud resources for additional volumes

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

NetApp storage efficiency features and storage costs

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

Capacity allocation decisions that Cloud Manager automatically handles

- Cloud Manager purchases additional EBS disks as capacity thresholds are exceeded. This

happens as your volumes grow.

- Cloud Manager deletes unused sets of EBS disks if the disks contain no volumes for 12 hours.
- Cloud Manager moves volumes between sets of disks to avoid capacity issues.

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

3.5. High-availability pairs

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

3.5.1. Overview

Cloud Volumes ONTAP HA configurations include the following components:

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



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

Storage takeover and giveback

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

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

RPO and RTO

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

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

HA deployment models

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

3.5.2. Cloud Volumes ONTAP HA in multiple Availability Zones

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

NFS and CIFS data access for clients within the VPC

When an HA configuration is spread across multiple Availability Zones, three floating IP addresses are required for NAS data access from within the VPC. The floating IP addresses, which must be outside of the CIDR blocks for all VPCs in the region, can migrate between nodes when failures occur.

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

You should review requirements for floating IP addresses and route tables before you deploy an HA configuration across multiple Availability Zones. You must specify the floating IP addresses when you deploy the configuration.

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

NFS and CIFS data access for clients outside the VPC

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

iSCSI data access

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

Storage takeover and giveback for iSCSI

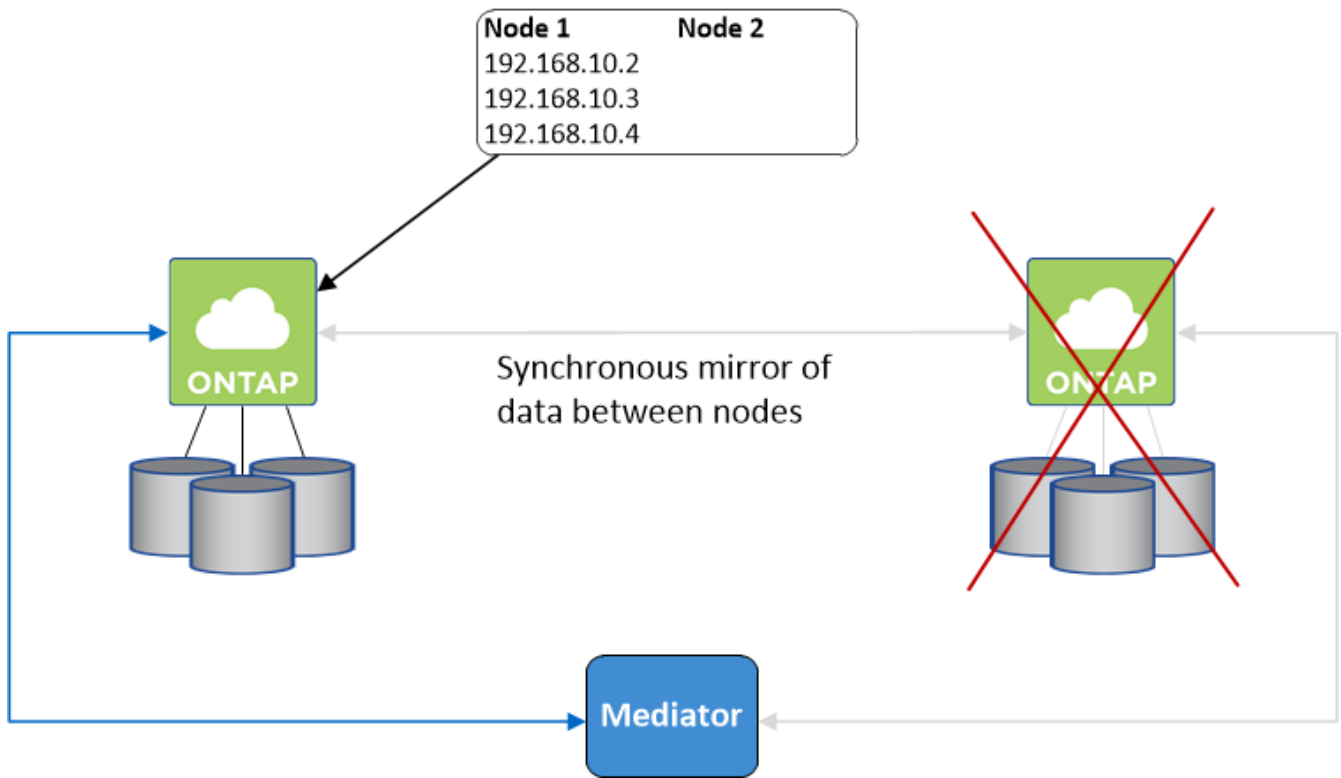
For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



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

Storage takeover and giveback for NAS

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



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

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

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

3.5.3. Cloud Volumes ONTAP HA in a single Availability Zone

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

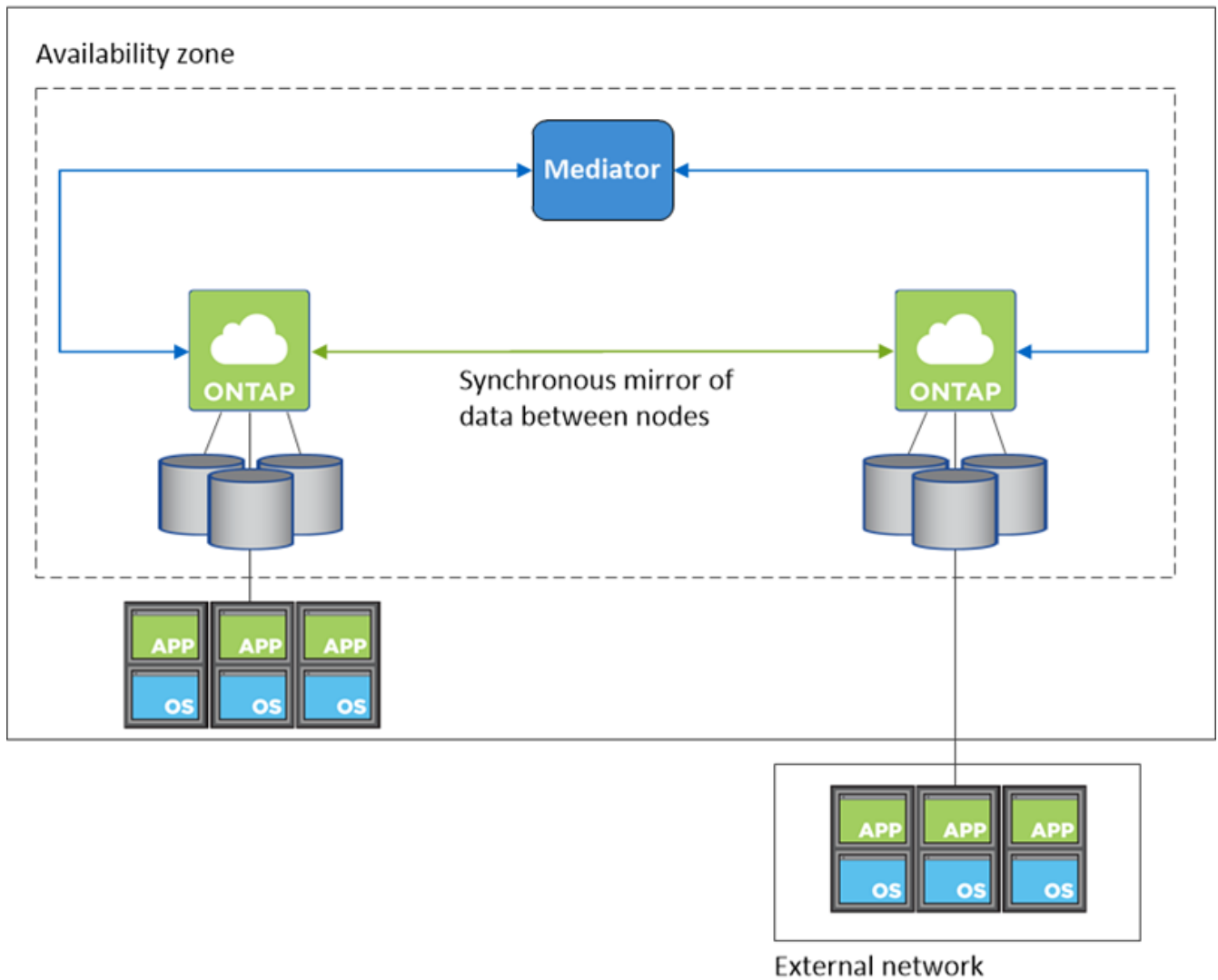


This HA configuration is not supported in the Volume View.

Data access

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

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



Storage takeover and giveback

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



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

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

3.5.4. How storage works in an HA pair

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

Storage allocation

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

Storage configurations

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



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

Performance expectations for an HA configuration

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

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

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

Client access to storage

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



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

You can easily identify the correct IP address from Cloud Manager. The following image shows the Storage System View:

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

The following image shows the Volume View:

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

3.6. Security

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

3.6.1. Data encryption in Azure

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



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

3.6.2. Data encryption in AWS

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

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

3.6.3. ONTAP virus scanning

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

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

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

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

3.7. WORM storage

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

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

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

Activating WORM storage

You can activate WORM storage on a Cloud Volumes ONTAP system when you create a new working environment. This includes specifying an activation code and setting the default retention period for files. You can obtain an activation code by using the chat icon in the lower right of the Cloud Manager interface.



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

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

[Shows the WORM option that is available when creating a new working environment.]

Committing files to WORM

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

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



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

Limitations

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

3.8. Licensing

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

License management for a new system

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

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

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

NetApp and installs it on the Cloud Volumes ONTAP system.

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

License expiration

Cloud Manager warns you 30 days before a license is due to expire and again when the license expires. The following image shows a 30-day expiration warning:

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

You can select the working environment to review the message.

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



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

License renewal

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

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

3.9. Performance

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

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

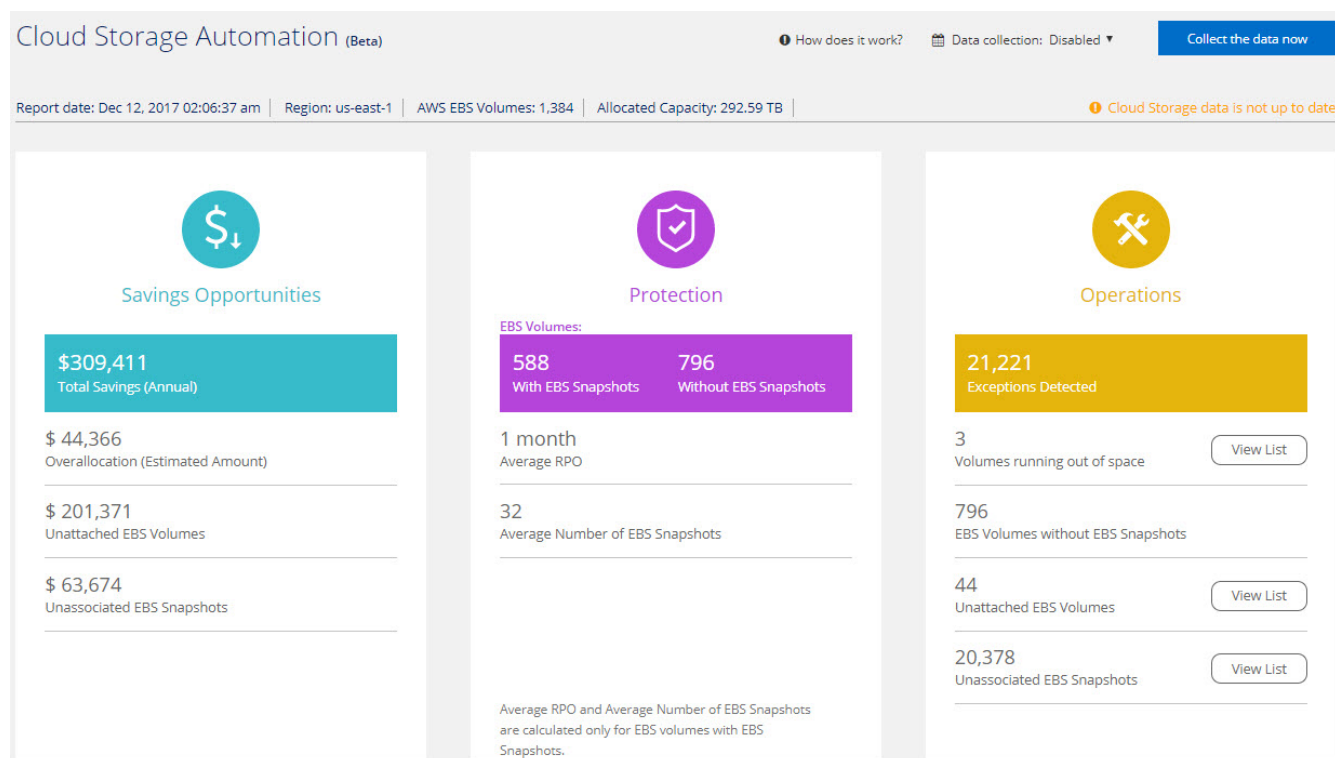
For Cloud Volumes ONTAP for Microsoft Azure, refer to [NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads](#).

3.10. Cloud Storage Automation

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

3.10.1. Sample report

The following image shows a sample report:



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

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

3.10.2. What happens when you enable the report

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

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

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

3.10.3. Required permissions

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

4. Getting started

4.1. Deployment overview

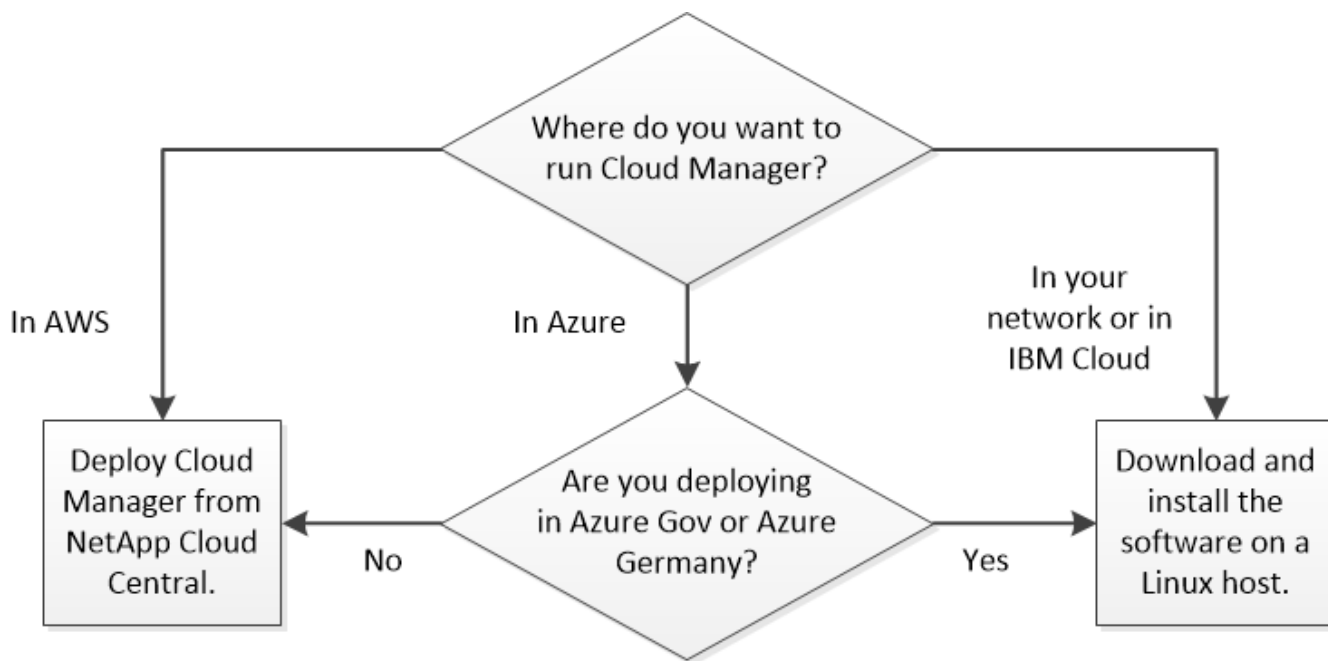
Before you get started, you might want to better understand your options for deploying OnCommand Cloud Manager and Cloud Volumes ONTAP.

4.1.1. Cloud Manager installation

Cloud Manager software is required to deploy and manage Cloud Volumes ONTAP. You can deploy Cloud Manager in any of the following locations:

- Amazon Web Services (AWS)
- Microsoft Azure
- IBM Cloud
- In your own network

How you deploy Cloud Manager depends on which location you choose:



Refer to the following for deploying Cloud Manager from NetApp Cloud Central:

- [Getting started in AWS](#)
- [Getting started in Azure](#)

For all other scenarios, refer to the following:

- [Installing Cloud Manager in an Azure US Gov region](#)
- [Installing Cloud Manager in the Azure Germany region](#)
- [Installing Cloud Manager on a Linux host](#)

4.1.2. Cloud Manager setup

You might want to perform additional setup after you install Cloud Manager, such as adding additional AWS accounts, installing an HTTPS certificate, and more. For instructions, see [Setting up Cloud Manager](#).

4.1.3. Cloud Volumes ONTAP deployment

After you get Cloud Manager up and running, you can start deploying Cloud Volumes ONTAP in AWS and in Microsoft Azure.

[Getting started in AWS](#) and [Getting started in Azure](#) provide instructions for getting Cloud Volumes ONTAP up and running quickly. For additional help, refer to the following:

- [Supported configurations for Cloud Volumes ONTAP 9.4](#)
- [Planning your configuration](#)
- [Launching Cloud Volumes ONTAP in AWS](#)
- [Launching Cloud Volumes ONTAP in Azure](#)

4.2. Getting started with Cloud Volumes ONTAP in AWS

You can get started with Cloud Volumes ONTAP in AWS by completing a few quick steps.



Set up your networking

- a. Enable outbound internet access from the target VPC so Cloud Manager and Cloud Volumes ONTAP can contact several endpoints.

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

- b. 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 from the AWS Marketplace

Subscribing from [the AWS Marketplace](#) is required to accept the software terms. You should only subscribe from the Marketplace. Launching Cloud Volumes ONTAP from anywhere but Cloud Manager is not supported.

3

Provide the required AWS permissions

When you deploy Cloud Manager from NetApp Cloud Central, you need to use an AWS account that has permissions to deploy the instance.

- a. Go to the AWS IAM console and create a policy by copying and pasting the contents of the [NetApp-provided JSON file](#).
- b. Attach the policy to the IAM user.

4

Launch Cloud Manager from NetApp Cloud Central

Cloud Manager software is required to deploy and manage Cloud Volumes ONTAP. It takes just a few minutes to launch a Cloud Manager instance from [Cloud Central](#).

5

Launch Cloud Volumes ONTAP using Cloud Manager

Once Cloud Manager is ready, just click Create, select the type of system that you would like to launch, and complete the steps in the wizard. After 25 minutes, your first Cloud Volumes ONTAP system should be up and running.

Watch the following video for a walk through of these steps:

► <https://www.youtube.com/watch?v=au5qQDiPuzo> (YouTube video)

Related links

- [Networking requirements for Cloud Manager](#)
- [Networking requirements for Cloud Volumes ONTAP in AWS](#)
- [Security group rules for AWS](#)
- [Setting up Cloud Manager](#)
- [Launching Cloud Volumes ONTAP in AWS](#)

4.3. Getting started with Cloud Volumes ONTAP in Azure

You can get started with Cloud Volumes ONTAP in Azure by completing a few quick steps. Separate instructions are available to deploy Cloud Manager in [US Gov regions](#) and in [Azure Germany regions](#).

1

Set up your networking

Enable outbound internet access from the target VNet so Cloud Manager and Cloud Volumes ONTAP can contact several endpoints.

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



Provide the required Azure permissions

When you deploy Cloud Manager from NetApp Cloud Central, you need to use an Azure account that has permissions to deploy the Cloud Manager virtual machine.

- a. Download the [NetApp-provided JSON file](#).
- b. Modify the JSON file by adding your Azure subscription ID to the "AssignableScopes" field.
- c. Use the JSON file to create a custom role in Azure named *Azure SetupAsService*.

```
Example:          az          role          definition          create          --role-definition
C:\Policy_for_Setup_As_Service_Azure.json
```

- d. From the Azure portal, assign the custom role to the user who will deploy Cloud Manager from Cloud Central.



Launch Cloud Manager from NetApp Cloud Central

Cloud Manager software is required to deploy and manage Cloud Volumes ONTAP. It takes just a few minutes to launch a Cloud Manager instance from [Cloud Central](#).



Launch Cloud Volumes ONTAP using Cloud Manager

Once Cloud Manager is ready, just click Create, select the type of system that you would like to deploy, and complete the steps in the wizard. After 25 minutes, your first Cloud Volumes ONTAP system should be up and running.

Watch the following video for a walk through of these steps:

► <https://www.youtube.com/watch?v=S2gP6ii9LAU> (YouTube video)

Related links

- [Networking requirements for Cloud Manager](#)
- [Networking requirements for Cloud Volumes ONTAP in Azure](#)
- [Security group rules for Azure](#)
- [Setting up Cloud Manager](#)
- [Launching Cloud Volumes ONTAP in Azure](#)

4.4. Setting up Cloud Manager

You can start creating Cloud Volumes ONTAP systems right after you deploy

Cloud Manager. However, you might want to perform additional setup first by setting up the AWS Key Management Service, installing an HTTPS certificate, and more.

4.4.1. Adding additional Azure subscriptions to Cloud Manager

If you want to deploy Cloud Volumes ONTAP systems in multiple Azure subscriptions, then you must add permissions for those subscriptions.

About this task

The following steps apply if you deployed Cloud Manager from NetApp Cloud Central. When you deployed Cloud Manager, Cloud Central created the OnCommand Cloud Manager Operator role and assigned it to the Cloud Manager virtual machine.

Steps

1. Log in to the Azure portal.
2. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.
3. Click **Access control (IAM)**.
4. Click **Add** and then add the permissions:
 - Select the **OnCommand Cloud Manager Operator** role.
 - Assign access to a **Virtual Machine**.
 - Select the subscription in which the Cloud Manager virtual machine was created.
 - Select the Cloud Manager virtual machine.
 - Click **Save**.
5. Repeat these steps for additional subscriptions.

Result

When you create a new working environment, you should now have the ability to select from multiple Azure subscriptions.

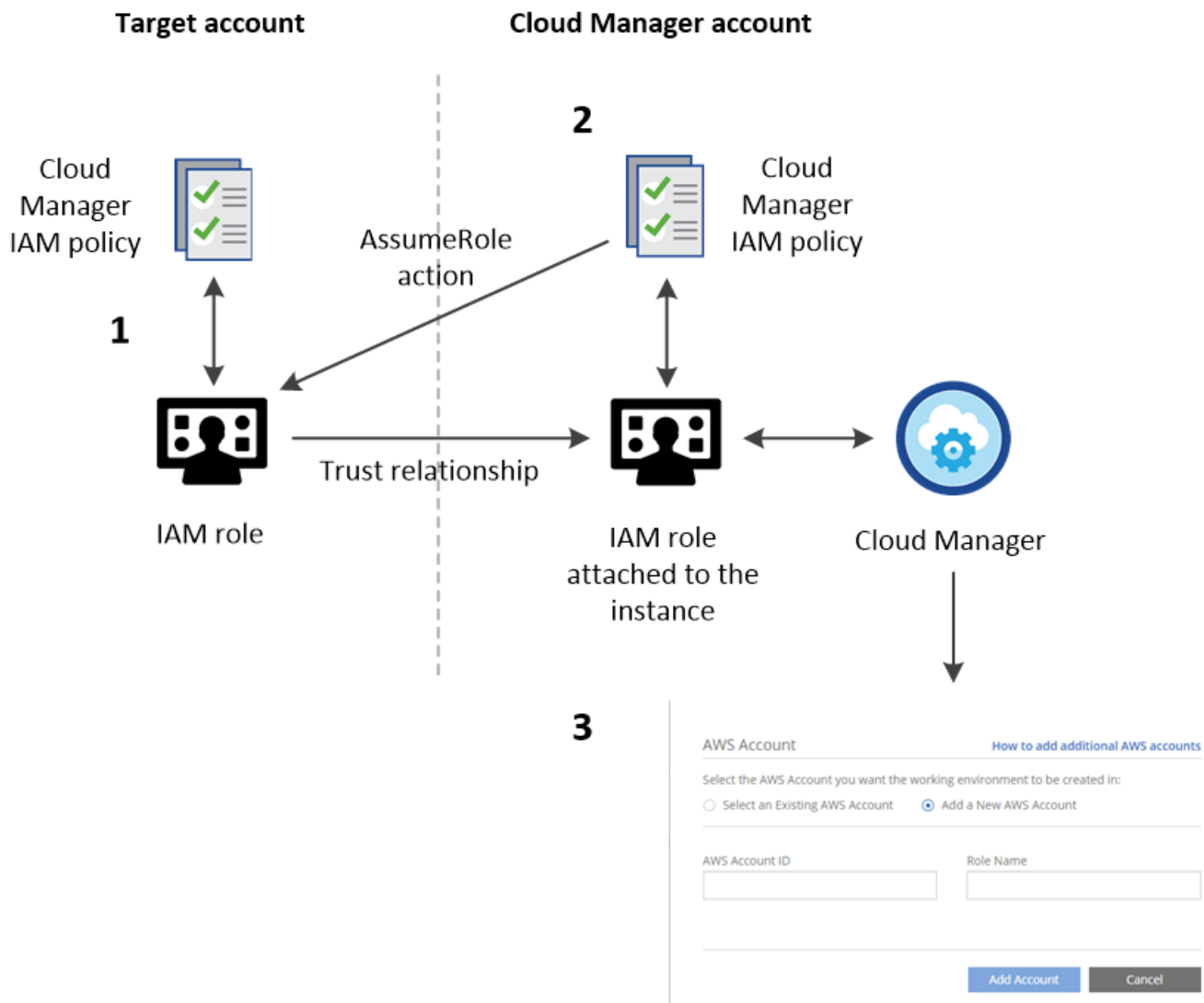
[Shows the Details and Credentials page in the create new working environment wizard. A link is available to select a different Azure subscription.]

4.4.2. Adding additional AWS accounts to Cloud Manager

When Cloud Manager is associated with an IAM role, it deploys Cloud Volumes ONTAP in the AWS account from which the Cloud Manager instance was created. If you want to deploy Cloud Volumes ONTAP in other AWS accounts, then you must delegate access across accounts.

About this task

The following image depicts the steps that you must complete below.



Steps

1. Create an IAM role in the AWS account in which you want to deploy Cloud Volumes ONTAP.

The role must meet the following requirements:

- It must adhere to [Cloud Manager IAM policy requirements](#).
- It must have a trust relationship that allows the IAM role associated with the Cloud Manager instance to assume this new role.

2. Add a permission to the Cloud Manager IAM role policy that enables it to assume the IAM role that you just created.



You can find the name of the Cloud Manager IAM role from the EC2 console by viewing a description of the instance.

3. When you create a new working environment, add the target account in the Details & Credentials page by specifying the AWS account ID of the target account and the name of the IAM role in that account.



As always, you must ensure network connectivity between Cloud Manager and the location of the target Cloud Volumes ONTAP systems. This is important when the instances are created by different accounts.

For additional background about this process, refer to [AWS Documentation: Tutorial: Delegate Access Across AWS Accounts Using IAM Roles](#). In this tutorial, the production account is similar to the target account and the development account is similar to the Cloud Manager account.

After you finish

If you have additional accounts, complete these steps for those accounts, as well.

4.4.3. Setting up the AWS KMS

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

Steps

1. Ensure that an active CMK exists in your account.

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

2. Add the IAM role associated with 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.

4.4.4. Installing an HTTPS certificate for secure access

By default, Cloud Manager uses a self-signed certificate for HTTPS access to the web console. You can install a certificate signed by a certificate authority (CA), which provides better security protection than a self-signed certificate.

Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **HTTPS Setup**.
2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

Option	Description
Generate a CSR	<p>a. Enter the host name or DNS of the Cloud Manager host (its Common Name), and then click Generate CSR.</p> <p>Cloud Manager displays a certificate signing request.</p> <p>b. Use the CSR to submit an SSL certificate request to a CA.</p> <p>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.</p> <p>c. Copy the contents of the signed certificate, paste it in the Certificate field, and then click Install.</p>
Install your own CA-signed certificate	<p>a. Select Install CA-signed certificate.</p> <p>b. Load both the certificate file and the private key and then click Install.</p> <p>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.</p>

Result

Cloud Manager now uses the CA-signed certificate to provide secure HTTPS access. The following image shows a Cloud Manager system that is configured for secure access:

[Screen shot: Shows the HTTPS Setup page after you install a signed certificate. The page shows the certificate properties and an option to renew the certificate.]

4.4.5. Adding users to Cloud Manager

If additional users need to use your Cloud Manager system, they must sign up for an account in NetApp Cloud Central. You can then add the users to Cloud Manager.

Steps

1. If the user does not yet have an account in NetApp Cloud Central, send them a link to your Cloud Manager system and have them sign up.

Wait until the user confirms that they have signed up for an account.

2. In Cloud Manager, click the user icon and then click **View Users**.
3. Click **New User**.
4. Enter the email address associated with the user account, select a role, and click **Add**.

After you finish

Inform the user that they can now log in to the Cloud Manager system.

4.4.6. Linking tenants to a NetApp Support Site account

You should link a tenant to a NetApp Support Site account so Cloud Manager can manage licenses for BYOL systems, register pay-as-you-go instances for support, and upgrade Cloud Volumes ONTAP software. For more information about these benefits, [watch this video](#).

Before you begin

Each NetApp Support Site account that you link to a tenant must meet the following requirements:

- The account must be a NetApp customer-level account (not a guest or temp account).
- If you purchased a secure BYOL subscription, then a *secure* NetApp Support Site account is required to upload the license file.

Contact your NetApp account team for further information about secure BYOL subscriptions.

- The account must be authorized to access the serial numbers of any BYOL systems deployed in the tenant.

If you do not have an account, you can create one from the [NetApp Support Site](#).

Steps

1. Click the tenants icon and then click **Switch Tenant**.

[Screen shot: Shows the tenant icon (a push pin) and the Switch Tenant button]

2. Click the edit icon for the tenant that you want to link to a NetApp Support Site account.

[Screen shot: Shows the edit icon (a pencil) which is available when hovering over a tenant.]

3. Click **Change NSS account**.
4. Enter the user name and password for the account and click **Save**.

Result

Cloud Manager registers all existing and future Cloud Volumes ONTAP systems in the tenant with NetApp support.

4.4.7. Setting up AWS billing and cost management for Cloud Manager

Cloud Manager can display the monthly compute and storage costs associated with running Cloud Volumes ONTAP in AWS. Before Cloud Manager can display the costs, users of AWS payer accounts must set up AWS to store billing reports in an S3 bucket, Cloud Manager must have permissions to access that S3 bucket, and AWS report tags must be enabled after you launch your first Cloud Volumes ONTAP instance.

Before you begin

You must have granted AWS permissions to Cloud Manager so it can access an S3 bucket. For details, see [Granting AWS permissions to Cloud Manager](#).

About this task

Users of AWS payer accounts must set up AWS to store billing reports in an S3 bucket. Cloud Manager uses the information from the reports to show monthly compute and storage costs associated with a Cloud Volumes ONTAP instance, as well as storage cost savings from NetApp product efficiency features (if they are enabled). For an example, see [Monitoring AWS storage and compute costs](#).

Steps

1. Go to the Amazon S3 console and set up an S3 bucket for the detailed billing reports:
 - a. Create an S3 bucket.
 - b. Apply a resource-based bucket policy to the S3 bucket to allow Billing and Cost Management to deposit the billing reports into the S3 bucket.

For details about using an S3 bucket for detailed billing reports and to use an example bucket policy, see [AWS Documentation: Understand Your Usage with Detailed Billing Reports](#).

2. From the Billing and Cost Management console, go to Preferences and enable the reports:
 - a. Enable **Receive Billing Reports** and specify the S3 bucket.
 - b. Enable **Cost allocation report**.
3. When you set up a user account in Cloud Manager, specify the S3 bucket that you created.



If you grant AWS permissions to Cloud Manager by specifying AWS keys, you must set up a Cloud Manager user account by specifying AWS keys for an IAM user created under the payer account or the AWS keys for the payer account itself.

4. After you launch your first Cloud Volumes ONTAP instance, go back to Billing and Cost Management **Preferences**, click **Manage report tags**, and enable the **WorkingEnvironmentId** tag.

This tag is not available in AWS until you create your first Cloud Volumes ONTAP working environment using any account under the AWS payer account.

Result

Cloud Manager updates the cost information at each 12-hour polling interval.

After you finish

Repeat these steps for other AWS payer accounts for which cost reporting is needed. For details about how to view the cost information, see [Monitoring AWS storage and compute costs](#).

4.5. Detailed networking requirements

4.5.1. Networking requirements for Cloud Manager

You must set up your networking so that Cloud Manager can deploy Cloud

Volumes ONTAP systems in AWS or in Microsoft Azure. 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, Cloud Manager prompts you to specify the proxy during setup. You can also specify the proxy server from the Settings page. Refer to [Configuring Cloud Manager to use a proxy server](#).

Connection to target networks

Cloud Manager requires a network connection to the AWS VPCs and Azure VNets in which you want to deploy Cloud Volumes ONTAP.

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

Outbound internet access

Cloud Manager requires outbound internet access to deploy and manage Cloud Volumes ONTAP. Outbound internet access is also required when accessing Cloud Manager from your web browser and when running the Cloud Manager installer on a Linux host.

The following sections identify the specific endpoints.

Outbound internet access to manage Cloud Volumes ONTAP in AWS

Cloud Manager requires outbound internet access to contact the following endpoints when deploying and managing Cloud Volumes ONTAP in AWS:

Endpoints	Purpose
<p>AWS services (amazonaws.com):</p> <ul style="list-style-type: none">• CloudFormation• Elastic Compute Cloud (EC2)• Key Management Service (KMS)• Security Token Service (STS)• Simple Storage Service (S3) <p>The exact endpoint depends on the region in which you deploy Cloud Volumes ONTAP. Refer to AWS documentation for details.</p>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in AWS.
api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.
cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.

Endpoints	Purpose
cognito-idp.us-east-1.amazonaws.com cognito-identity.us-east-1.amazonaws.com	Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
https://mysupport.netapp.com	Communication with NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Communication with NetApp for licensing and support registration.
<p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Third-party locations are subject to change.</p>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

Outbound internet access to manage Cloud Volumes ONTAP in Azure

Cloud Manager requires outbound internet access to contact the following endpoints when deploying and managing Cloud Volumes ONTAP in Microsoft Azure:

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions.
https://management.microsoftazure.de https://login.microsoftonline.de	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure US Gov regions.
api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.
cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
cognito-idp.us-east-1.amazonaws.com cognito-identity.us-east-1.amazonaws.com sts.amazonaws.com	Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.

Endpoints	Purpose
kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
https://mysupport.netapp.com	Communication with NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Communication with NetApp for licensing and support registration.
<p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Third-party locations are subject to change.</p>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

Outbound internet access from your web browser

Users must access Cloud Manager from a web browser. The machine running the web browser must have connections to the following endpoints:

Endpoints	Purpose
The Cloud Manager host	<p>You must enter the host's IP address from a web browser to load the Cloud Manager console.</p> <p>If you deploy Cloud Manager in AWS, the easiest way to provide access is by allocating a public IP address. However, if you want to use a private IP address instead, users can access the console through either of the following:</p> <ul style="list-style-type: none"> • A jump host in the VPC that has a connection to Cloud Manager • A host in your network that has a VPN connection to the private IP address
https://auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central.

Outbound internet access to install Cloud Manager on a Linux host

The Cloud Manager installer must access the following URLs during the installation process:

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

Ports and security groups

- If you deploy Cloud Manager from Cloud Central or from the marketplace images, refer to the following:
 - [Security group rules for Cloud Manager in AWS](#)
 - [Security group rules for Cloud Manager in Azure](#)
- If you install Cloud Manager on an existing Linux host, see [Cloud Manager host requirements](#).

4.5.2. Networking requirements for Cloud Volumes ONTAP in AWS

You must set up your AWS networking so Cloud Volumes ONTAP systems can operate properly.

Looking for the list of endpoints to which Cloud Manager requires access? They're now maintained in a single location. [Click here for details](#).

General AWS networking requirements for Cloud Volumes ONTAP

The following requirements must be met in AWS.

Outbound internet access for Cloud Volumes ONTAP nodes

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

Routing and firewall policies must allow AWS HTTP/HTTPS traffic to mysupport.netapp.com.

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.

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 \(AWS PrivateLink\)](#).

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 from Cloud Volumes ONTAP to AWS S3 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 in other networks

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

DNS and Active Directory for CIFS

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

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

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

AWS networking requirements for Cloud Volumes ONTAP HA 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.

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.

Floating IP addresses for NAS data access

Cloud Volumes ONTAP HA configurations in multiple AZs use floating IP addresses for NAS client access from within the VPC. These IP addresses can migrate between nodes when failures occur.

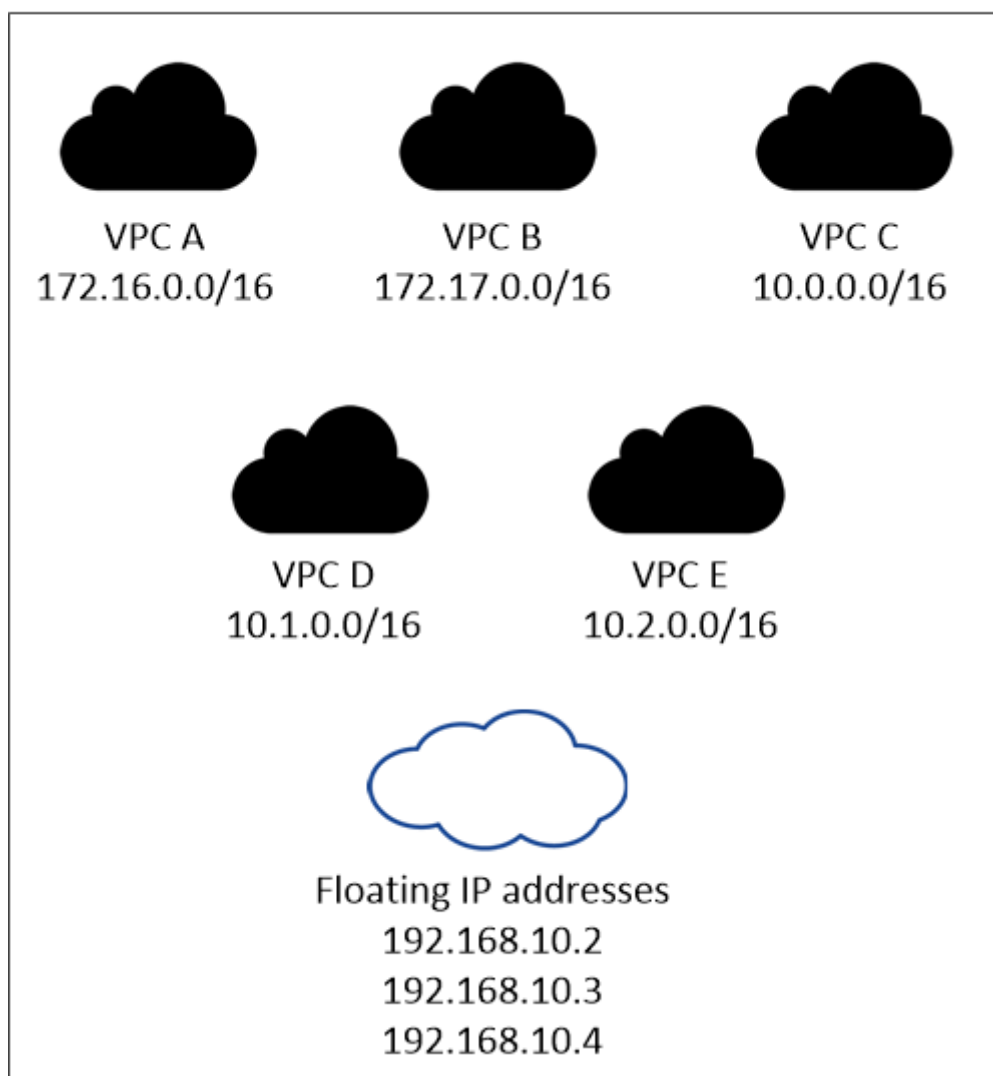
You must specify three floating IP addresses that are outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. You can think of the floating IP addresses as a logical subnet that is outside of the VPCs in your region.



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.

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 are routable to subnets through route tables.

AWS region



You must manually 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.



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

Floating IP address for SVM management

If you use SnapDrive for Windows or SnapCenter with an HA pair, a floating IP address is also required for the SVM management LIF. Cloud Manager prompts you to specify the IP address when you launch the HA pair. If you did not specify the IP address, you can create the SVM Management LIF later. For details, see [Setting up Cloud Volumes ONTAP](#).

Route tables

After you specify the floating IP addresses in Cloud Manager, you must 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 is 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 cannot access the HA pair.

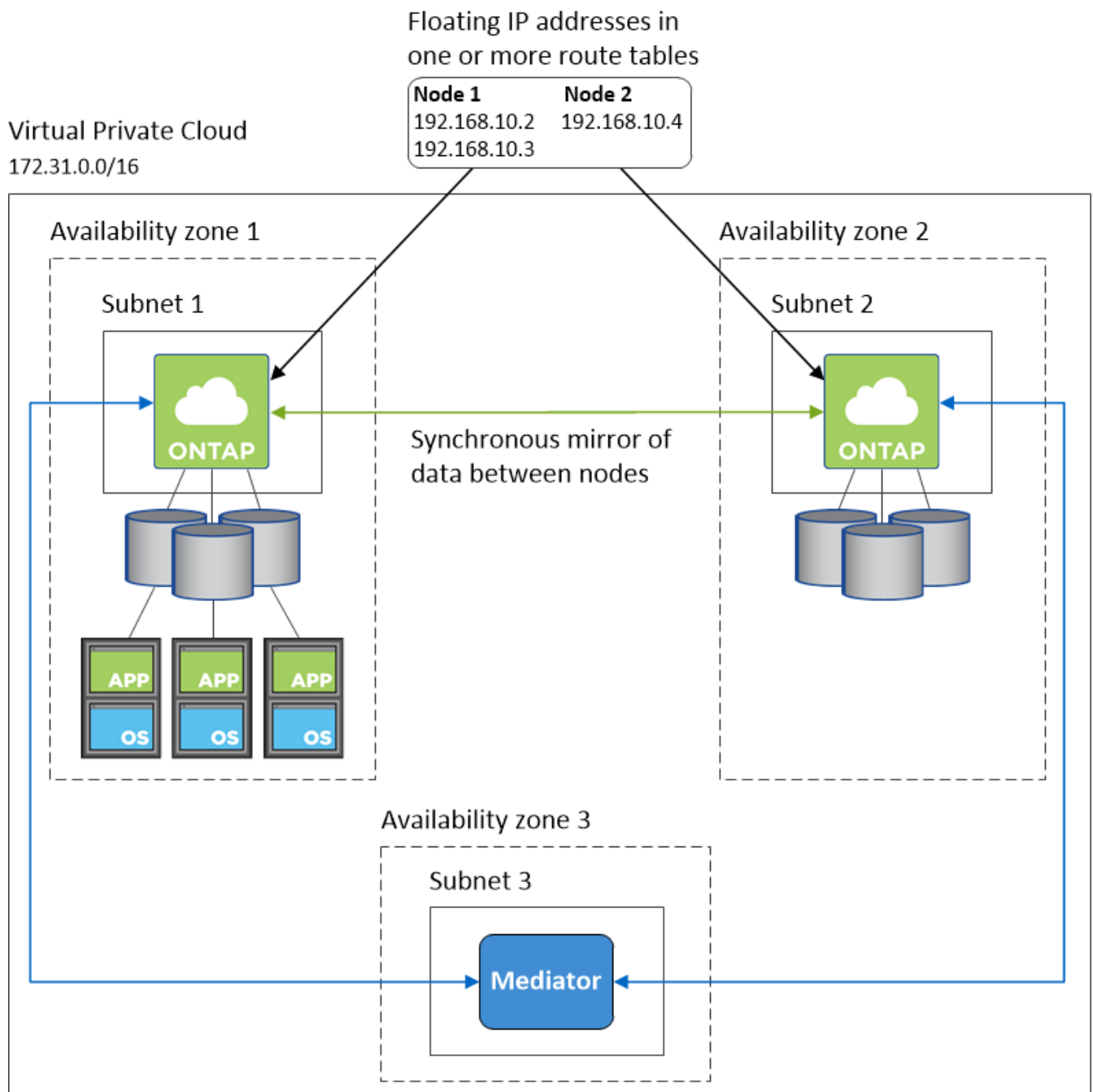
For more information about route tables, refer to [AWS Documentation: Route Tables](#).

Connection to NetApp management tools

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. If you want to use NetApp management tools with HA configurations, they must be in the same VPC with similar routing configuration as NAS clients.

Example configuration

The following image shows an optimal HA configuration in AWS operating as an active-passive configuration:



Sample VPC configurations

To better understand how you can deploy Cloud Manager and Cloud Volumes ONTAP in AWS, you should review the most common VPC configurations.

- A VPC with public and private subnets and a NAT device
- A VPC with a private subnet and a VPN connection to your network

A VPC with public and private subnets and a NAT device

This VPC configuration includes public and private subnets, an internet gateway that connects the VPC to the internet, and a NAT gateway or NAT instance in the public subnet that enables outbound internet traffic from the private subnet. In this configuration, you can run Cloud Manager in a public subnet or private subnet, but the public subnet is recommended because it allows access from hosts outside the VPC. You can then launch Cloud Volumes ONTAP instances in the private

subnet.

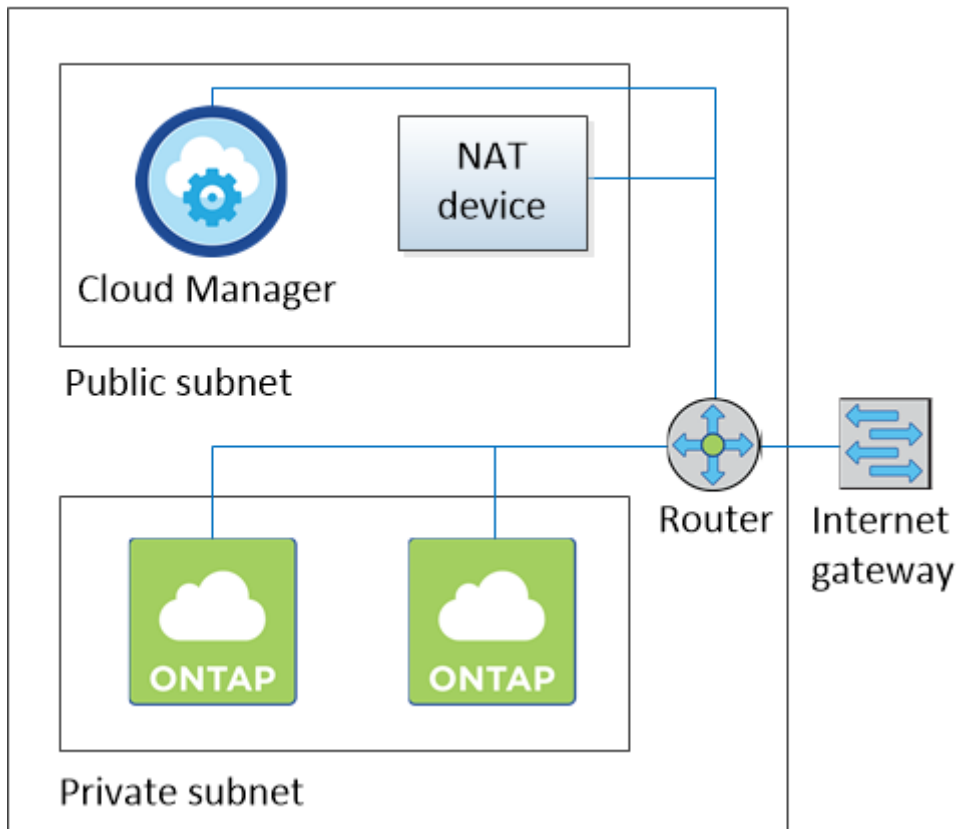


Instead of a NAT device, you can use an HTTP proxy to provide internet connectivity.

For more details about this scenario, refer to [AWS Documentation: Scenario 2: VPC with Public and Private Subnets \(NAT\)](#).

The following graphic shows Cloud Manager running in a public subnet and single node systems running in a private subnet:

Virtual Private Cloud



A VPC with a private subnet and a VPN connection to your network

This VPC configuration is a hybrid cloud configuration in which Cloud Volumes ONTAP becomes an extension of your private environment. The configuration includes a private subnet and a virtual private gateway with a VPN connection to your network. Routing across the VPN tunnel allows EC2 instances to access the internet through your network and firewalls. You can run Cloud Manager in the private subnet or in your data center. You would then launch Cloud Volumes ONTAP in the private subnet.

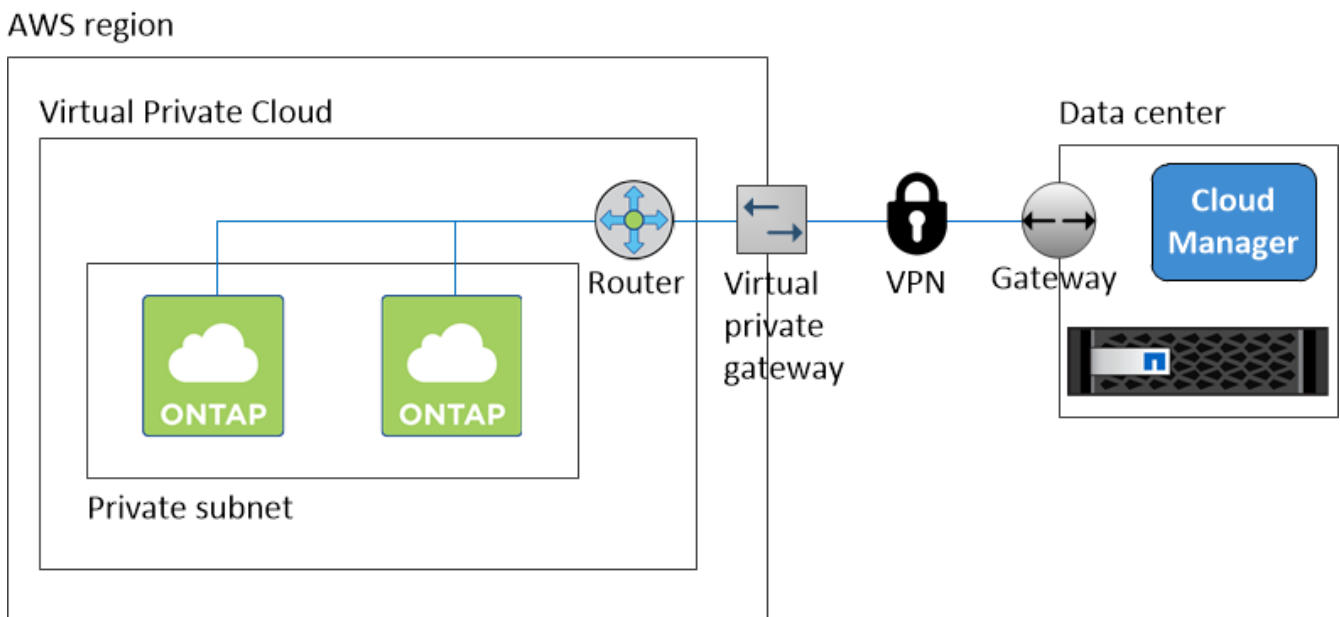


You can also use a proxy server in this configuration to allow internet access. The proxy server can be in your data center or in AWS.

If you want to replicate data between FAS systems in your data center and Cloud Volumes ONTAP systems in AWS, you should use a VPN connection so that the link is secure.

For more details about this scenario, refer to [AWS Documentation: Scenario 4: VPC with a Private Subnet Only and AWS Managed VPN Access](#).

The following graphic shows Cloud Manager running in your data center and single node systems running in a private subnet:



4.5.3. Networking requirements for Cloud Volumes ONTAP in Azure

You must set up your Azure networking so Cloud Volumes ONTAP systems can operate properly.

Looking for the list of endpoints to which Cloud Manager requires access? They're now maintained in a single location. [Click here for details](#).

Outbound internet access for Cloud Volumes ONTAP

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

Routing and firewall policies must allow Azure HTTP/HTTPS traffic to [mysupport.netapp.com](#) so Cloud Volumes ONTAP can send AutoSupport messages.

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 from Cloud Volumes ONTAP to Azure Blob storage for data tiering

If you want to tier cold data to Azure Blob storage, you do not need to set up a VNet service endpoint as long as Cloud Manager has the required permission:

"Microsoft.Network/virtualNetworks/subnets/write",

That permission is included in the latest Cloud Manager policy. For details about providing permissions, see [Granting Azure permissions](#).

For details about setting up data tiering, see [Tiering cold data to low-cost object storage](#).



If your network configuration uses route tables, then Cloud Manager also requires the following permission: Microsoft.Network/routeTables/join/action

Connections to ONTAP systems in other networks

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

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

4.6. Additional deployment options

4.6.1. Cloud Manager host requirements

If you install Cloud Manager on your own host, then you must verify support for your configuration, which includes operating system requirements, port requirements, and so on.

Supported AWS EC2 instance types

t2.medium or m4.large

Supported Azure VM sizes

A2 or D2_v2

Supported operating systems

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4

The Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during Cloud Manager installation.

Cloud Manager is supported on English-language versions of these operating systems.

Hypervisor

A bare metal or hosted hypervisor that is certified to run CentOS or Red Hat Enterprise Linux

[Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?](#)

CPU

2.27 GHz or higher with two cores

RAM

4 GB

Free disk space

50 GB

Outbound internet access

Outbound internet access is required when installing Cloud Manager and when using Cloud Manager to deploy Cloud Volumes ONTAP. For a list of endpoints, see [Networking requirements for Cloud Manager](#).

Ports

The following ports must be available:

- 80 for HTTP access
- 443 for HTTPS access
- 3306 for the Cloud Manager database
- 8080 for the Cloud Manager API proxy

If other services are using these ports, Cloud Manager installation fails.



There is a potential conflict with port 3306. If another instance of MySQL is running on the host, it uses port 3306 by default. You must change the port that the existing MySQL instance uses.

You can change the default HTTP and HTTPS ports when you install Cloud Manager. You cannot change the default port for the MySQL database. If you change the HTTP and HTTPS ports, you must ensure that users can access the Cloud Manager web console from a remote host:

- Modify the security group to allow inbound connections through the ports.
- Specify the port when you enter the URL to the Cloud Manager web console.

4.6.2. Installing Cloud Manager on an existing Linux host

If you want to run the Cloud Manager software on an existing host, you can download and install the software on a Linux host in your network or in the cloud.

Before you begin

- A Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during Cloud Manager installation.
- The Cloud Manager installer accesses several URLs during the installation process. You must ensure that outbound internet access is allowed to those endpoints. Refer to [Networking requirements for Cloud Manager](#).

About this task

- Root privileges are not required to install Cloud Manager.
- Cloud Manager installs the AWS command line tools (awscli) to enable recovery procedures from NetApp support.

If you receive a message that installing the awscli failed, you can safely ignore the message. Cloud Manager can operate successfully without the tools.

Steps

1. Review networking requirements:
 - [Networking requirements for Cloud Manager](#)
 - [Networking requirements for Cloud Volumes ONTAP for AWS](#)
 - [Networking requirements for Cloud Volumes ONTAP for Azure](#)
2. Set up permissions for Cloud Manager:
 - a. If you want to deploy Cloud Volumes ONTAP in AWS, [set up an IAM role that includes the required permissions](#).
 - b. If you want to deploy Cloud Volumes ONTAP in Azure, [create and set up a service principal in Azure Active Directory](#).
3. Review [Cloud Manager host requirements](#).
4. Download the software from the [NetApp Support Site](#), and then copy it to the Linux host.

For help with connecting and copying the file to an EC2 instance in AWS, see [AWS Documentation: Connecting to Your Linux Instance Using SSH](#).

5. Assign permissions to execute the script.

Example

```
chmod +x OnCommandCloudManager-V3.5.0.sh
```

6. Run the installation script:

```
./OnCommandCloudManager-V3.5.0.sh [silent] [proxy=ipaddress] [proxyport=port]  
[proxyuser=user_name] [proxypwd=password]
```

silent runs the installation without prompting you for information.

proxy is required if the Cloud Manager host is behind a proxy server.

proxyport is the port for the proxy server.

proxyuser is the user name for the proxy server, if basic authentication is required.

proxypwd is the password for the user name that you specified.

7. Unless you specified the *silent* parameter, type **Y** to continue the script, and then enter the HTTP and HTTPS ports when prompted.

If you change the HTTP and HTTPS ports, you must ensure that users can access the Cloud Manager web console from a remote host:

- Modify the security group to allow inbound connections through the ports.
- Specify the port when you enter the URL to the Cloud Manager web console.

Cloud Manager is now installed. At the end of the installation, the Cloud Manager service (occm) restarts twice if you specified a proxy server.

8. Open a web browser and enter the following URL:

`https://ipaddress:port`

ipaddress can be localhost, a private IP address, or a public IP address, depending on the configuration of the Cloud Manager host. For example, if Cloud Manager is in the public cloud without a public IP address, you must enter a private IP address from a host that has a connection to the Cloud Manager host.

port is required if you changed the default HTTP (80) or HTTPS (443) ports. For example, if the HTTPS port was changed to 8443, you would enter `https://ipaddress:8443`

9. Sign up for a NetApp Cloud Central account or log in if you already have one.
10. When you sign up or log in, Cloud Manager automatically adds your user account as the administrator for this system.
11. After you log in, enter a name for this Cloud Manager system.

After you finish

You can start creating Cloud Volumes ONTAP systems but you might want to perform additional setup first.

4.6.3. Launching Cloud Manager from the AWS Marketplace

It is best to launch Cloud Manager in AWS using [NetApp Cloud Central](#), but you can launch it from the AWS Marketplace, if needed.



If you launch Cloud Manager from the AWS Marketplace, Cloud Manager is still integrated with NetApp Cloud Central. [Learn more about the integration.](#)

Before you begin

If you want to assign a public IP address to the Cloud Manager instance and use the AWS 1-Click Launch option, the public subnet must be already enabled to automatically assign public IP addresses. Otherwise, you must use the Manual Launch option to assign a public IP address to the instance.

For details, refer to [AWS Documentation: IP Addressing in Your VPC](#).

Steps

1. Set up an IAM role that includes the required permissions.

[Granting permissions when Cloud Manager is not launched from Cloud Central](#)

2. Go to the [Cloud Manager page on the AWS Marketplace](#).
3. Click **Continue**.
4. Launch the instance from the 1-Click Launch tab or the Custom Launch tab, depending on how you want to grant AWS permissions to Cloud Manager:

Choice	Steps
You want to associate the instance with an IAM role.	<ol style="list-style-type: none">a. On the Custom Launch tab, click Launch with EC2 Console for your region.b. Choose the t2.medium or m4.large instance type.c. Select a VPC, subnet, IAM role, and other configuration options that meet your requirements.d. Keep the default storage options.e. Enter tags for the instance, if desired.f. Specify the required connection methods for the Cloud Manager instance: SSH, HTTP, and HTTPS.g. Click Launch.
You do not want to associate the instance with an IAM role. You want to specify AWS keys for each Cloud Manager user account.	<ol style="list-style-type: none">a. On the 1-Click Launch tab, specify settings for the instance. Note the following:<ul style="list-style-type: none">◦ The t2.medium and m4.large instance types are supported.◦ Under security group, select Create new based on seller settings to create a pre-defined security group that includes the rules required by Cloud Manager.b. Click Accept Terms and Launch with 1-Click.

Result

AWS launches the software with the specified settings. The Cloud Manager instance and software should be running in approximately five minutes.

After you finish

Log in to Cloud Manager by entering the public IP address or private IP address in a web browser and then complete the Setup wizard.

4.6.4. Deploying Cloud Manager from the Azure Marketplace

It is best to deploy Cloud Manager in Azure using [NetApp Cloud Central](#), but you can deploy it from the Azure Marketplace, if needed.



If you deploy Cloud Manager from the Azure Marketplace, Cloud Manager is still integrated with NetApp Cloud Central. [Learn more about the integration.](#)

Deploying Cloud Manager in Azure

You need to install and set up Cloud Manager so you can use it to launch Cloud Volumes ONTAP in Azure.

Steps

1. [Go to the Azure Marketplace page for Cloud Manager.](#)
2. Click **Get it now** and then click **Continue**.
3. From the Azure portal, click **Create** and follow the steps to configure the virtual machine.

Note the following as you configure the virtual machine:

- Cloud Manager can perform optimally with either HDD or SSD disks.
- You should choose one of the recommended virtual machine sizes: A2 or D2_v2.
- For the network security group, it is best to choose **Advanced**.

The **Advanced** option creates a new security group that includes the required inbound rules for Cloud Manager. If you choose Basic, refer to [Security group rules](#) for the list of required rules.

- Under the settings, enable **Managed Service Identity** for Cloud Manager by selecting **Yes**.

This setting is important because a Managed Service Identity allows a Cloud Manager virtual machine to identify itself to Azure Active Directory without providing any credentials. This method is simpler than [manually setting up an Azure service principal and providing the credentials to Cloud Manager](#).

For more information about Managed Service Identities, refer to [Azure documentation](#).

4. On the summary page, review your selections and click **Create** to start the deployment.

Azure deploys the virtual machine with the specified settings. The virtual machine and Cloud Manager software should be running in approximately five minutes.

5. Open a web browser from a host that has a connection to the Cloud Manager virtual machine and enter the following URL:

`http://ipaddress:80`

When you log in, Cloud Manager automatically adds your user account as the administrator for this system.

6. After you log in, enter a name for the Cloud Manager system.

Result

Cloud Manager is now installed and set up. You must grant Azure permissions before users can deploy Cloud Volumes ONTAP in Azure.

Granting Azure permissions to Cloud Manager

When you deployed Cloud Manager in Azure, you should have enabled a Managed Service Identity. You must now grant the required Azure permissions by creating a custom role and then by assigning the role to the Cloud Manager virtual machine for one or more subscriptions.

Steps

1. Create a custom role using the Cloud Manager policy:
 - a. Download the [Cloud Manager Azure policy](#).
 - b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

You should add the ID for each Azure subscription from which users will create Cloud Volumes ONTAP systems.

Example

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- c. Use the JSON file to create a custom role in Azure.

The following example shows how to create a custom role using the Azure CLI 2.0:

```
az           role           definition           create           --role-definition  
C:\Policy_for_Cloud_Manager_Azure_3_5_2.json
```

You should now have a custom role called OnCommand Cloud Manager Operator that you can assign to the Cloud Manager virtual machine.

2. Assign the role to the Cloud Manager virtual machine for one or more subscriptions:
 - a. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.
 - b. Click **Access control (IAM)**.

c. Click **Add** and then add the permissions:

- Select the **OnCommand Cloud Manager Operator** role.



OnCommand Cloud Manager Operator is the default name provided in the [Cloud Manager policy](#). If you chose a different name for the role, then select that name instead.

- Assign access to a **Virtual Machine**.
- Select the subscription in which the Cloud Manager virtual machine was created.
- Select the Cloud Manager virtual machine.
- Click **Save**.

d. If you want to deploy Cloud Volumes ONTAP from additional subscriptions, switch to that subscription and then repeat these steps.

Result

Cloud Manager now has the permissions that it needs to deploy and manage Cloud Volumes ONTAP in Azure.

4.6.5. Installing Cloud Manager in an Azure US Gov region

To deploy Cloud Manager in an Azure US Gov region, you must download the Cloud Manager installer from the NetApp Support Site and install it on an existing CentOS 7.3 host.

About this task

For a list of supported Azure US Gov regions, see [Supported Azure regions](#).

Steps

1. [Review networking requirements for Azure](#).
2. Create a CentOS 7.3 virtual machine from the Azure Marketplace.

While Cloud Manager supports other operating systems, it only supports CentOS 7.3 in the Azure US Gov regions.

3. [Download and install Cloud Manager](#).
4. [Grant Azure permissions to Cloud Manager using a service principal and credentials](#).



Managed Service Identities are not supported in the US Gov regions.

After you finish

Cloud Manager is now ready to deploy Cloud Volumes ONTAP in an Azure US Gov region, just like any other region. However, you might want to perform additional setup first.

4.6.6. Installing Cloud Manager in an Azure Germany region

The Azure Marketplace is not available in the Azure Germany regions, so you must download the Cloud Manager installer from the NetApp Support Site and install it on an existing Linux host in the region.

Steps

1. [Review networking requirements for Azure.](#)
2. [Review Cloud Manager host requirements.](#)
3. [Download and install Cloud Manager.](#)
4. [Grant Azure permissions to Cloud Manager using a service principal and credentials.](#)



Managed Service Identities are not supported in the Azure Germany regions.

After you finish

Cloud Manager is now ready to deploy Cloud Volumes ONTAP in the Azure Germany region, just like any other region. However, you might want to perform additional setup first.

4.7. Additional ways to provide permissions

4.7.1. Granting permissions when Cloud Manager is not launched from Cloud Central

If you cannot launch Cloud Manager in AWS from [NetApp Cloud Central](#), then you must provide Cloud Manager with the permissions that it needs if you want to launch and manage Cloud Volumes ONTAP in AWS.

About this task

The Cloud Manager IAM policy defines the AWS actions and resources that Cloud Manager is allowed to use. You can grant the permissions defined in the IAM policy in one of two ways:

- You can attach an IAM role to the Cloud Manager instance in AWS.
- You can attach the IAM policy to IAM users or groups.

You would then specify the AWS access keys for those users in Cloud Manager.

Steps

1. Download the Cloud Manager IAM policy from the following location:

[NetApp OnCommand Cloud Manager: AWS and Azure Policies](#)

2. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.
3. Grant permissions to the Cloud Manager instance or to IAM users:

Option	Description
Grant permissions to the Cloud Manager instance	<ol style="list-style-type: none"> Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role. Attach the IAM role to Cloud Manager when you launch it from the AWS Marketplace (choose Custom Launch) or by modifying an existing instance from the EC2 console.
Grant permissions to IAM users	Attach the policy to IAM users or groups. For instructions, refer to AWS Documentation: Managing IAM Policies .

Result

Cloud Manager now has the permissions that it needs. If you attached the policy to IAM users, you must specify the AWS access keys for those IAM users when you set up user accounts in Cloud Manager.

4.7.2. Granting Azure permissions to Cloud Manager using a service principal and credentials

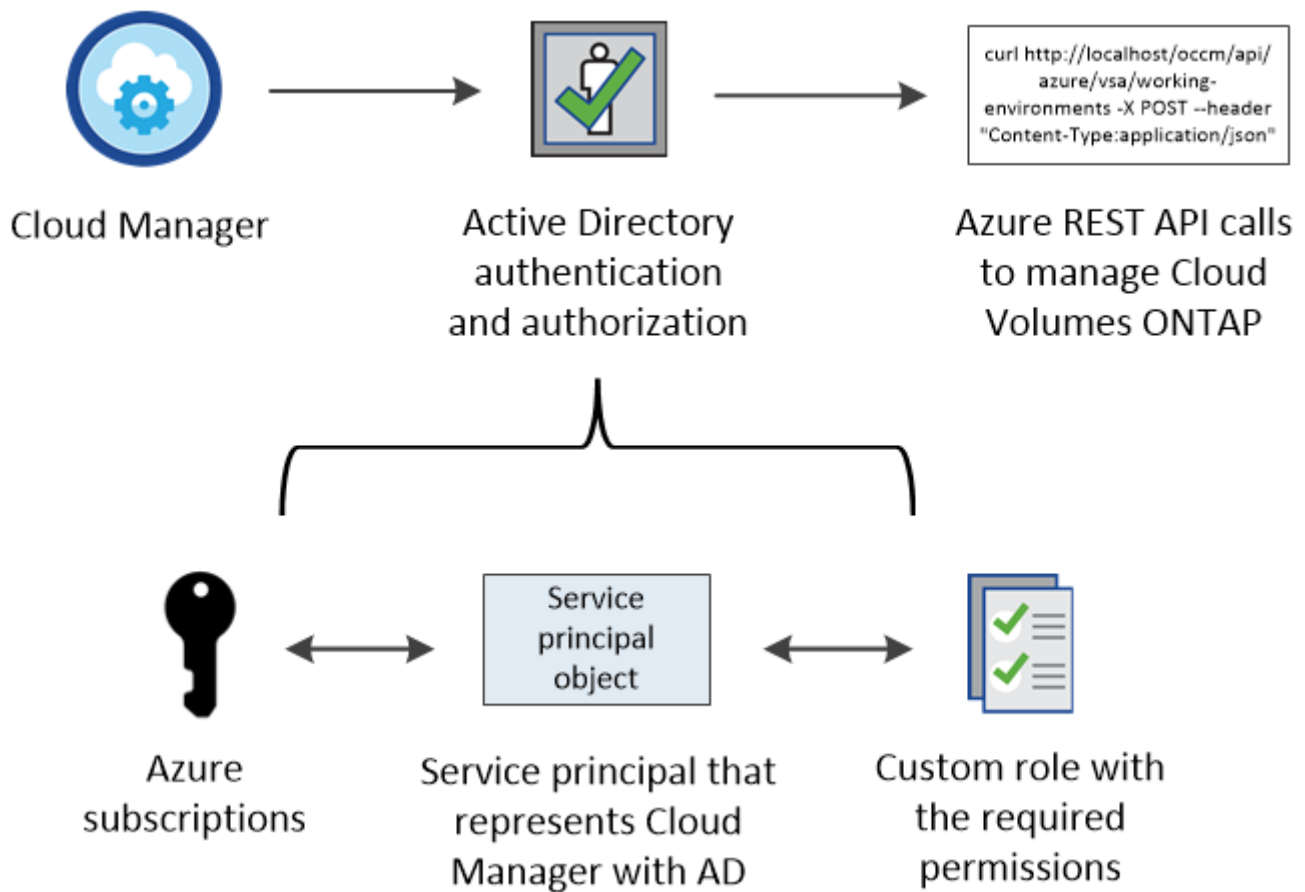
Cloud Manager needs permissions to perform actions in Azure. You can grant the required permissions by creating and setting up a service principal in Azure Active Directory and by obtaining the Azure credentials that Cloud Manager needs.

Before you begin

Using a service principal and credentials is an alternative to using a Managed Service Identity, which is simpler and does not require credentials. To use a Managed Service Identity with Cloud Manager instead, follow [instructions for new Cloud Manager virtual machines](#) or [instructions for existing Cloud Manager virtual machines](#).

About this task

The following image depicts how Cloud Manager obtains permissions to perform operations in Azure. A service principal object, which is tied to one or more Azure subscriptions, represents Cloud Manager in Azure Active Directory and is assigned to a custom role that allows the required permissions.



The following steps use the new Azure portal. If you experience any issues, you should use the Azure classic portal.

Steps

1. [Create a custom role with the required Cloud Manager permissions.](#)
2. [Create an Active Directory service principal.](#)
3. [Assign the custom Cloud Manager Operator role to the service principal.](#)

Creating a custom role with the required Cloud Manager permissions

A custom role is required to provide Cloud Manager with the permissions that it needs to launch and manage Cloud Volumes ONTAP in Azure.

Steps

1. Download the [Cloud Manager Azure policy](#).
2. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

You should add the ID for each Azure subscription from which users will create Cloud Volumes ONTAP systems.

Example

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
```

```
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzzz"
```

3. Use the JSON file to create a custom role in Azure.

The following example shows how to create a custom role using the Azure CLI 2.0:

```
az role definition create --role-definition C:\Policy_for_Cloud_Manager_Azure_3_5_2.json
```

Result

You should now have a custom role called OnCommand Cloud Manager Operator.

Creating an Active Directory service principal

You must create an Active Directory service principal so Cloud Manager can authenticate with Azure Active Directory.

Before you begin

You must have the appropriate permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to [Microsoft Azure Documentation: Use portal to create Active Directory application and service principal that can access resources](#)

Steps

1. From the Azure portal, open the **Azure Active Directory** service.

[Shows the Active Directory service in Microsoft Azure.]

2. In the menu, click **App registrations**.

3. Create the service principal:

- a. Click **New application registration**.

- b. Enter a name for the application, keep **Web app / API** selected, and then enter any URL—for example, <http://url>

- c. Click **Create**.

4. Modify the application to add the required permissions:

- a. Select the created application.

- b. Under Settings, click **Required permissions** and then click **Add**.

[Shows the settings for an Active Directory application in Microsoft Azure and highlights the option to add required permissions for API access.]

- c. Click **Select an API**, select **Windows Azure Service Management API**, and then click **Select**.

[Shows the API to select in Microsoft Azure when adding API access to the Active Directory application. The API is the Windows Azure Service Management API.]

- d. Click **Access Azure Service Management as organization users**, click **Select** and then click **Done**.

5. Create a key for the service principal:

- a. Under Settings, click **Keys**.
- b. Enter a description, select a duration, and then click **Save**.
- c. Copy the key value.

You need to enter the key value in Cloud Manager when you create user accounts for this subscription.

- d. Click **Properties** and then copy the application ID for the service principal.

Similar to the key value, you need to enter the application ID in Cloud Manager when you create user accounts for this subscription.

[Shows the application ID for an Azure Active Directory service principal.]

6. Obtain the Active Directory tenant ID for your organization:

- a. In the Active Directory menu, click **Properties**.
- b. Copy the Directory ID.

[Shows the Active Directory properties in the Azure portal and the Directory ID that you need to copy.]

Just like the application ID and application key, you must enter the Active Directory tenant ID when you create Cloud Manager user accounts.

Result

You should now have an Active Directory service principal and you should have copied the application ID, the application key, and the Active Directory tenant ID. You need to enter this information in Cloud Manager when you set up user accounts.

Assigning the Cloud Manager Operator role to the service principal

You must bind the service principal to one or more Azure subscriptions and assign it the Cloud Manager Operator role so Cloud Manager has permissions in Azure.

About this task

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. Cloud Manager enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

Steps

1. From the Azure portal, select **Subscriptions** in the left pane.
2. Select the subscription.
3. Click **Access control (IAM)** and then click **Add**.
4. Select the **OnCommand Cloud Manager Operator** role.
5. Search for the name of the application (you cannot find it in the list by scrolling).

6. Select the application, click **Select**, and then click **OK**.

Result

The service principal for Cloud Manager now has the required Azure permissions.

4.7.3. Providing Azure permissions to an existing Cloud Manager virtual machine using a Managed Service Identity

You can provide Azure permissions to Cloud Manager by using a Managed Service Identity. A Managed Service Identity allows the Cloud Manager virtual machine to identify itself to Azure Active Directory without providing any credentials.



Managed Service Identities are not supported in the Azure US Gov regions and in the Germany regions. You must [grant Azure permissions to Cloud Manager using a service principal and credentials](#).

About this task

If you currently provide Cloud Manager with Azure permissions through a service principal, you can change to using a Managed Service Identity instead. This method is simpler than manually setting up an Azure service principal and providing the credentials to Cloud Manager.

For more information about Managed Service Identities, refer to [Azure documentation](#).

Steps

1. Log in to the Azure portal using an account that is associated with the Cloud Manager virtual machine.
2. Enable a Managed Service Identity on the virtual machine:
 - a. Navigate to the virtual machine.
 - b. Under Settings, select **Configuration**.
 - c. Click **Yes** next to Managed Service Identity and then click **Save**.
3. Provide permissions to the Cloud Manager virtual machine for one or more subscriptions:
 - a. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.
 - b. Click **Access control (IAM)**.
 - c. Click **Add** and then add the permissions:
 - Select the **OnCommand Cloud Manager Operator** role.



OnCommand Cloud Manager Operator is the default name provided in the [Cloud Manager policy](#). If you chose a different name for the role, then select that name instead.

If you have not yet created this role, follow [these instructions](#).

- Assign access to a **Virtual Machine**.
 - Select the subscription in which the Cloud Manager virtual machine was created.
 - Select the Cloud Manager virtual machine.
 - Click **Save**.
- d. If you want to deploy Cloud Volumes ONTAP from additional subscriptions, click **Subscriptions** again, select a subscription, and then repeat the steps for that subscription.

Result

Cloud Manager now has permissions that are controlled by a Managed Service Identity. If you repeated the steps for several subscriptions, then you can choose a different subscription when creating a new working environment.

[Screen shot: Shows the link to select a different subscription in the Details and Credentials page.]

5. Deploying Cloud Volumes ONTAP

5.1. Before you create Cloud Volumes ONTAP systems

Before you use Cloud Manager to create and manage Cloud Volumes ONTAP systems, your Cloud Manager administrator should have prepared networking and installed and set up Cloud Manager.

Your administrator should have followed instructions to get up and running [in AWS](#) or [in Azure](#), and optionally [set up Cloud Manager](#).

The following conditions should exist before you start deploying Cloud Volumes ONTAP:

- AWS and Azure networking requirements were met for Cloud Manager and Cloud Volumes ONTAP.
- Cloud Manager has permissions to perform operations in AWS and Azure on your behalf.
- Each Cloud Volumes ONTAP product that users will deploy was subscribed to from the AWS Marketplace.
- Cloud Manager was installed.
- (Optional) Additional tenants were defined.
- (Optional) Additional user accounts were created, which can include Tenant Admins and Working Environment Admins.

5.2. Logging in to Cloud Manager

You can log in to Cloud Manager from any web browser that has a connection to the Cloud Manager system. You should log in using a [NetApp Cloud Central](#) user account.

Steps

1. Open a web browser and log in to [NetApp Cloud Central](#).
2. Click **Go to Cloud Data Services** and select **Cloud Volumes ONTAP**.
3. Click **Go to Cloud Manager** for the Cloud Manager system that you want to access.



If you do not see any systems listed, make sure that the Cloud Manager administrator added your NetApp Cloud Central account to the system.

4. Log in to Cloud Manager using your NetApp Cloud Central account.

[The log in screen for Cloud Manager.]

5.3. Planning your Cloud Volumes ONTAP configuration

When you deploy Cloud Volumes ONTAP, 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.

5.3.1. Choosing a license type

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

- [Supported configurations for Cloud Volumes ONTAP 9.4](#)
- [Supported configurations for ONTAP Cloud 9.3](#)

5.3.2. Understanding storage limits

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

- [Storage limits for Cloud Volumes ONTAP 9.4](#)
- [Storage limits for ONTAP Cloud 9.3](#)

5.3.3. Choosing an AWS disk type

When you create volumes for Cloud Volumes ONTAP, you need to choose the underlying cloud storage that Cloud Volumes ONTAP uses as a disk. In AWS, you can choose a single EBS disk type or a tiered storage configuration that uses EBS storage as a performance tier and S3 as a capacity tier. You should choose the configuration that meets your requirements for performance and cost.

For an overview of data tiering, see [Storage](#). For requirements, see [Tiering data in AWS](#).

Supported EBS disk types

At a high level, the differences between EBS disk types are as follows:

- *General Purpose SSD* disks balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS.
- *Provisioned IOPS SSD* disks are for critical applications that require the highest performance at a higher cost.
- *Throughput Optimized HDD* disks are for frequently accessed workloads that require fast and consistent throughput at a lower price.
- *Cold HDD* disks are meant for backups, or infrequently accessed data, because the performance

is very low. Like Throughput Optimized HDD disks, performance is defined in terms of throughput.



Cold HDD disks are not supported with HA configurations.

For additional details about the use cases for these disks, refer to [AWS Documentation: EBS Volume Types](#).

5.3.4. Choosing an Azure disk type

When you create volumes for Cloud Volumes ONTAP, you need to choose the underlying cloud storage that Cloud Volumes ONTAP uses as a disk. In Azure, you can choose a managed disk or a tiered storage configuration that uses managed disks as a performance tier and Azure Blob storage as a capacity tier. You should choose the configuration that meets your requirements for performance and cost.

For an overview of data tiering, see [Storage](#). For requirements, see [Tiering cold data to low-cost object storage](#).

Supported Azure managed disks

The underlying managed disk type for Azure can be Premium Storage or Standard Storage:

- *Premium Storage* disks store data on solid state drives (SSDs). The SSD disks provide high performance for I/O-intensive workloads at a higher cost.
- If you do not need high IOPS, you can reduce your costs by using *Standard Storage* disks which are backed by hard disk drives (HDD).

For additional details about the use cases for these disks, see [Microsoft Azure Documentation: Introduction to Microsoft Azure Storage](#).

5.3.5. Choosing a disk size

You can choose from several disk sizes when you launch Cloud Volumes ONTAP and when you use the advanced allocation option. You should consider the disk size carefully because it impacts cost, performance, and total volume and system capacity.

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



In AWS, Cloud Manager gradually increases the size of disks as a system grows. For details, see [Disk size selection for aggregates in AWS](#).

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

Different disk sizes are available for each disk type. Note that all disks in an aggregate must be the same size.

How disk size relates to performance in AWS

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.

Larger disks have a higher baseline and burst performance, so you should always consider performance along with cost. Ultimately, you should choose the disk size that gives you the *sustained performance* that you need.

For example, when using General Purpose SSD disks, you might choose the following disk sizes:

- 100 GB because you want to start out with something small or because you have low performance requirements
- 500 GB because you want to get the best price to performance ratio
- 4 TB because you need very high sustained IOPS performance

Even if you do choose larger disks (for example, six 4 TB disks), you might not get all of the IOPS because the EC2 instance can reach its bandwidth limit.

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

How disk size relates to performance in Azure

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

When sizing for performance, you should also be aware of performance limits tied to Azure virtual machine types. For details, refer to the following:

- [Microsoft Azure Documentation: High-performance Premium Storage and managed disks for VMs](#)
- [Microsoft Azure Documentation: Sizes for Linux virtual machines in Azure](#)

There are no performance differences between disk sizes for Standard Storage. You should choose disk size based on the capacity that you need.

5.3.6. Choosing a write speed

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

Difference between normal write speed and high write speed

When you choose normal write speed, data is written directly to disk, thereby reducing the likelihood of data loss in the event of an unplanned system outage.

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, AWS EBS volume performance 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.

Recommendations when using high write speed

If you enable high write speed, you should ensure write protection at the application layer.

5.3.7. Choosing a volume usage profile

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

NetApp storage efficiency features provide the following benefits:

Thin provisioning

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

Deduplication

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

Compression

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

5.3.8. AWS network information worksheet

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

Network information for Cloud Volumes ONTAP

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

Network information for an HA pair in multiple AZs

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

5.3.9. Azure network information worksheet

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

Azure information	Your value
Region	
Virtual network (VNet)	

Azure information	Your value
Subnet	
Network security group (if using your own)	

5.4. Launching Cloud Volumes ONTAP in AWS

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

5.4.1. Launching a single 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.

Before you begin

- 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](#).
- If you want to launch a BYOL system, you must have the 20-digit serial number (license key) and you must have credentials for a NetApp Support Site account, if the tenant is not already linked with an account.
- If you want to use CIFS, you must have set up DNS and Active Directory. For details, see [Networking requirements for Cloud Volumes ONTAP in AWS](#).

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 Working Environments page, click **Add Working Environment**.
2. Under Create, select **Cloud Volumes ONTAP**.
3. On the Details and Credentials page, optionally change the AWS account, 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
AWS Account	If you want to deploy Cloud Volumes ONTAP in other AWS accounts, then you must delegate access across accounts using an IAM role. For instructions, see Adding additional AWS accounts to Cloud Manager .
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Add tags	<p>AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance.</p> <p>You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment.</p> <p>For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.</p>
Credentials	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.



If AWS keys were not specified for your Cloud Manager account, you are prompted to enter them after you click Continue. You need to enter them before you can proceed.

- On the Location page, enter the network information that you recorded in the AWS worksheet and then click **Continue**.

The following image shows the Location page filled out:

[Screen shot: Shows the VPC page filled out for a new Cloud Volumes ONTAP instance.]

- On the Data Encryption page, choose no data encryption or AWS-managed encryption.

To better understand these options, see [Data encryption in AWS](#).

For AWS-managed encryption, you can choose a different master key if more than one key is available in your account.

- On the BYOL License page, specify whether you have a license for this Cloud Volumes ONTAP system.

To understand how licenses work, see [Licensing](#).

- On the Preconfigured Packages page, select one of the packages to quickly launch Cloud Volumes ONTAP, or click **Create my own configuration**.

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

8. On the IAM Role page, you should 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](#).

9. On the Licensing page, change the Cloud Volumes ONTAP version as needed, select a license, an instance type, the instance tenancy, and then click **Continue**.

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



If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.4 RC1 and 9.4 GA is available. The update does not occur from one release to another—for example, from 9.3 to 9.4.

10. If the NetApp Support Site credentials page is displayed, enter your NetApp Support Site credentials.

Credentials are required for BYOL instances. For details, see [Why you should link a tenant to your NetApp Support Site account](#).

11. On the Underlying Storage Resources page, choose a storage type and a disk size for all disks in the initial aggregate.

You can choose a different disk type for subsequent volumes. For help choosing a disk type, see [Choosing an AWS disk type](#).

For help choosing a disk size, see [Choosing a disk size](#).

12. On the Write Speed & WORM page, choose **Normal** or **High** write speed, and activate write once, read many (WORM) storage, if desired.

[Learn more about write speed.](#)

[Learn more about WORM storage.](#)

13. On the Create Volume page, enter details for the new volume, and then click **Continue**.

You might skip this step if you want to create a volume for iSCSI. Cloud Manager sets up volumes for NFS and CIFS only.

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.

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

[Screen shot: Shows the Volume page filled out for a Cloud Volumes ONTAP instance.]

- If you chose the CIFS protocol, set up a CIFS server on the CIFS Setup page:

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

15. On the Usage Profile, Disk Type, and Tiering Policy page, choose whether you want to enable storage efficiency features and edit the S3 tiering policy, if needed.

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

16. On the Review & Approve page, 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 launched a pay-as-you-go instance and the tenant is not linked to a NetApp Support Site account, manually register the instance with NetApp to enable support. For instructions, see [Registering Cloud Volumes ONTAP](#).

Support from NetApp is included with your Cloud Volumes ONTAP system. To activate support, you must first register the instance with NetApp.

- 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.

- If this is the first Cloud Volumes ONTAP instance launched in AWS, remind your administrator to finish [setting up AWS billing and cost management for Cloud Manager](#) by enabling the WorkingEnvironmentId tag. This tag is not available in AWS until after you create your first Cloud Volumes ONTAP working environment under the AWS payer account.

5.4.2. 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.

Before you begin

- 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](#).

- If you purchased BYOL licenses, you must have a 20-digit serial number (license key) for each node, and you must have credentials for a NetApp Support Site account if the tenant is not already associated with an account.
- If you want to use CIFS, you must have set up DNS and Active Directory. For details, see [Networking requirements for Cloud Volumes ONTAP in AWS](#).

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 Working Environments page, click **Add Working Environment**.
2. Under Create, select **Cloud Volumes ONTAP HA**.
3. On the Details and Credentials page, optionally change the AWS account, 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
AWS Account	If you want to deploy Cloud Volumes ONTAP in other AWS accounts, then you must delegate access across accounts using an IAM role. For instructions, see Adding additional AWS accounts to Cloud Manager .
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. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources .
Credentials	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.



If AWS keys were not specified for your Cloud Manager account, you are prompted to enter them after you click Continue. You must enter the AWS keys before you proceed.

4. On the HA Deployment Models page, choose an HA configuration.

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

5. On the Location page, enter the network information that you recorded in the AWS worksheet and then click **Continue**.

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

[Screen shot: Shows the VPC page filled out for an HA configuration. A different availability zone is selected for each instance.]

6. On the Connectivity and SSH Authentication page, choose connection methods for the HA pair and the mediator.
7. If you chose multiple AZs, specify the floating IP addresses and then click **Continue**.

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](#).

8. If you chose multiple AZs, select the route tables that should include routes to the floating IP addresses and then click **Continue**.

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](#).

9. On the Data Encryption page, choose no data encryption or AWS-managed encryption.

To better understand these options, see [Data encryption in AWS](#).

For AWS-managed encryption, you can choose a different master key if more than one key is available in your account.

10. On the BYOL License page, specify whether you have a license for this Cloud Volumes ONTAP system.

To understand how licenses work, see [Licensing](#).

11. On the Preconfigured Packages page, select one of the packages to quickly launch a Cloud Volumes ONTAP system, or click **Create my own configuration**.

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

12. On the IAM Role page, you should keep the default option to let Cloud Manager create the roles for you.

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

13. On the Licensing page, change the Cloud Volumes ONTAP version as needed, select a license, an instance type, the instance tenancy, and then click **Continue**.

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



If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.4 RC1 and 9.4 GA is available. The update does not occur from one release to another—for example, from 9.3 to 9.4.

14. If the NetApp Support Site credentials page is displayed, enter your NetApp Support Site credentials.

Credentials are required for BYOL instances. For details, see [Why you should link a tenant to your NetApp Support Site account](#).

15. On the Underlying Storage Resources page, choose a storage type and a disk size for all disks in the initial aggregate.

You can choose a different disk type for subsequent volumes. For help choosing a disk type, see [Choosing an AWS disk type](#).

For help choosing a disk size, see [Choosing a disk size](#).

16. On the WORM page, activate write once, read many (WORM) storage, if desired.

[Learn more about WORM storage](#).

17. On the Create Volume page, enter details for the new volume, and then click **Continue**.

You might skip this step if you want to create a volume for iSCSI. Cloud Manager sets up volumes for NFS and CIFS only.

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

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

Field	Description
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.

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

[Screen shot: Shows the Volume page filled out for a Cloud Volumes ONTAP instance.]

18. If you selected the CIFS protocol, set up a CIFS server on the CIFS Setup page:

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

19. On the Usage Profile, Disk Type, and Tiering Policy page, choose whether you want to enable storage efficiency features and edit the S3 tiering policy, if needed.

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

20. On the Review & Approve page, review and confirm your selections:
- Review details about the configuration.
 - Click **More information** to review details about support and the AWS resources that Cloud Manager will purchase.
 - Select the **I understand...** check boxes.
 - Click **Go**.

Result

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

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

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

After you finish

- If you launched a pay-as-you-go instance and the tenant is not linked to a NetApp Support Site account, manually register the instance with NetApp to enable support. For instructions, see [Registering Cloud Volumes ONTAP](#).

Support from NetApp is included with your Cloud Volumes ONTAP system. To activate support, you must first register the instance with NetApp.

- 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.

- If this is the first Cloud Volumes ONTAP instance launched in AWS, remind your administrator to finish [setting up AWS billing and cost management for Cloud Manager](#) by enabling the WorkingEnvironmentId tag. This tag is not available in AWS until after you create your first Cloud Volumes ONTAP working environment under the AWS payer account.

5.5. Launching Cloud Volumes ONTAP in Azure

You can launch a single Cloud Volumes ONTAP system in Azure by creating a Cloud Volumes ONTAP working environment in Cloud Manager.

Before you begin

- You should have prepared by choosing a configuration and by obtaining Azure networking information from your administrator. For details, see [Planning your Cloud Volumes ONTAP configuration](#).
- If you want to deploy a BYOL system, you must have the 20-digit serial number (license key) and you must have credentials for a NetApp Support Site account, if the tenant is not already linked with an account.

About this task

When Cloud Manager creates a Cloud Volumes ONTAP system in Azure, it creates a resource group that includes the security group, network interfaces, and two storage accounts: one for Azure Standard Storage and one for Premium Storage.

Steps

1. On the Working Environments page, click **Add Working Environment**
2. Under Create, select **Cloud Volumes ONTAP**.
3. On the Details and Credentials page, optionally change the Azure subscription, specify a cluster name and resource group name, add tags if needed, and then specify credentials.

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

Field	Description
Azure Subscription	You can choose a different Azure subscription if you provided permissions through multiple subscriptions. If you are using a Managed Service Identity, see Enabling a Managed Service Identity on an existing Cloud Manager virtual machine . If you are using a service principal with credentials, see Assigning the Cloud Manager Operator role to the service principal .
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the Azure virtual machine. It also uses the name as the prefix for the predefined security group, if you select that option.
Resource Group Name	If you uncheck Use Default , you can type the name of an existing resource group or a new resource group.
Tags	<p>Tags are metadata for your Azure resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP system and each Azure resource associated with the system.</p> <p>You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment.</p> <p>For information about tags, refer to Microsoft Azure Documentation: Using tags to organize your Azure resources.</p>
Credentials	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.



If Azure credentials were not specified for your Cloud Manager account, you are prompted to enter them after you click Continue. You need to enter them before you can proceed.

4. On the Location page, enter the network information that you recorded in the worksheet, select the checkbox to confirm network connectivity, and then click **Continue**.
5. On the BYOL License page, specify whether you have a license for this Cloud Volumes ONTAP system.

To understand how licenses work, see [Licensing](#).

6. On the Preconfigured Packages page, select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

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

7. On the Licensing page, change the Cloud Volumes ONTAP version as needed, select a license and a virtual machine type, and then click **Continue**.

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



If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.4 RC1 and 9.4 GA is available. The update does not occur from one release to another—for example, from 9.2 to 9.3.

8. On the Azure Marketplace page, follow the steps if Cloud Manager could not enable programmatic deployments of Cloud Volumes ONTAP.
9. If the NetApp Support Site credentials page is displayed, enter your NetApp Support Site credentials.

Credentials are required for BYOL instances. For details, see [Why you should link a tenant to your NetApp Support Site account](#).

10. On the Underlying Storage Resources page, choose either **Premium Storage** (SSD) or **Standard Storage** (HDD) and select a disk size.

The disk type is for the initial volume. You can choose a different disk type for subsequent volumes. For help choosing a disk type, see [Choosing an Azure disk type](#).

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

For help choosing a size, see [Choosing a disk size](#).

11. On the Write Speed & WORM page, choose **Normal** or **High** write speed, and activate write once, read many (WORM) storage, if desired.

[Learn more about write speed.](#)

[Learn more about WORM storage.](#)

12. On the Create Volume page, enter details for the new volume, and then click **Continue**.

You should skip this step if you want to use iSCSI. Cloud Manager enables you to create volumes for NFS and CIFS only.

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.

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

[Screen shot: Shows the Volume page filled out for a Cloud Volumes ONTAP instance.]

13. If you chose the CIFS protocol, set up a CIFS server on the CIFS Setup page:

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

Field	Description
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.

14. On the Usage Profile, Disk Type, and Tiering Policy page, choose whether you want to enable storage efficiency features and change the tiering policy, if needed.

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

15. On the Review & Approve page, review and confirm your selections:
 - a. Review details about the configuration.
 - b. Click **More information** to review details about support and the Azure resources that Cloud Manager will purchase.
 - c. Select the **I understand...** check boxes.
 - d. Click **Go**.

Result

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

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

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

After you finish

- If you deployed a pay-as-you-go system and the tenant is not linked to a NetApp Support Site account, manually register the system with NetApp to enable support. For instructions, see [Registering Cloud Volumes ONTAP](#).

Support from NetApp is included with your Cloud Volumes ONTAP system. To activate support, you must first register the system with NetApp.

- 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.

5.6. Registering pay-as-you-go systems

Support from NetApp is included with Cloud Volumes ONTAP Explore, Standard, and Premium systems, but you must first activate support by registering the systems with NetApp, if you have not set up automatic registration.

Before you begin

The host from which you are logged in to Cloud Manager must have internet access. If it does not, you can register from another location by going to [NetApp Cloud Volumes ONTAP Registration](#).

About this task

If a tenant is linked to a NetApp Support Site account, Cloud Manager automatically registers the system with that account. However, if the tenant is not linked to an account, then you should register systems with NetApp after you launch them.

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

Steps

1. On the Working Environments page, double-click the name of the system that you want to register.
2. Click the menu icon and then click **Support registration**:

[Screen shot: Shows the Support registration option selected in the menu icon for a Cloud Volumes ONTAP system.]

The information that you need to register an instance is displayed:

- Instance ID
 - Serial number
 - Account ID
3. To automatically register future instances in the tenant, click the link to enter your NetApp Support Site credentials.
 4. To register this instance with NetApp support, click the link and then click **Register to NetApp support**.

Following this link automatically completes the instance ID, serial number, and account ID in the registration form.

5. Follow the instructions to register your Cloud Volumes ONTAP system.

5.7. Setting up Cloud Volumes ONTAP

After you deploy Cloud Volumes ONTAP, you can set it up by synchronizing the system time using NTP and by performing a few optional tasks from either System Manager or the CLI.

Task	Description
Synchronize the system time using NTP	<p>Cloud Volumes ONTAP needs a Network Time Protocol (NTP) server to synchronize the time with clients and peered clusters. Problems can occur when the time is inaccurate.</p> <p>You can configure the NTP server using System Manager or the CLI. For instructions, see the System Manager Help or the ONTAP 9 System Administration Reference.</p>
Optional: Configure AutoSupport	<p>AutoSupport proactively monitors the health of your system and automatically sends messages to NetApp technical support by default.</p> <p>If the Cloud Manager Admin added a proxy server to Cloud Manager before you launched your instance, Cloud Volumes ONTAP is configured to use that proxy server for AutoSupport messages.</p> <p>You should test AutoSupport to ensure that it can send messages. For instructions, see the System Manager Help or the ONTAP 9 System Administration Reference.</p>
Optional: Configure EMS	<p>The Event Management System (EMS) collects and displays information about events that occur on Cloud Volumes ONTAP systems. To receive event notifications, you can set event destinations (email addresses, SNMP trap hosts, or syslog servers) and event routes for a particular event severity.</p> <p>You can configure EMS using the CLI. For instructions, see the ONTAP 9 EMS Configuration Express Guide.</p>
Optional: Create an SVM management network interface (LIF) for HA systems	<p>A storage virtual machine (SVM) management network interface (LIF) is required if you want to use SnapCenter or SnapDrive for Windows with an HA pair. The SVM management LIF must use a <i>floating</i> IP address when using an HA pair across multiple AWS Availability Zones.</p> <p>Cloud Manager prompts you to specify the floating IP address when you launch the HA pair. If you did not specify the IP address, you can create the SVM Management LIF yourself from System Manager or the CLI. The following example shows how to create the LIF from the CLI:</p> <pre>network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home -port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall-policy mgmt</pre>

Task	Description
Optional: Change the backup location of configuration files	<p>Cloud Volumes ONTAP automatically creates configuration backup files that contain information about the configurable options that it needs to operate properly.</p> <p>By default, Cloud Volumes ONTAP backs up the files to the Cloud Manager host every eight hours. If you want to send the backups to an alternate location, you can change the location to an FTP or HTTP server in your data center or in AWS. For example, you might already have a backup location for your FAS storage systems.</p> <p>You can change the backup location using the CLI. See the ONTAP 9 System Administration Reference.</p>

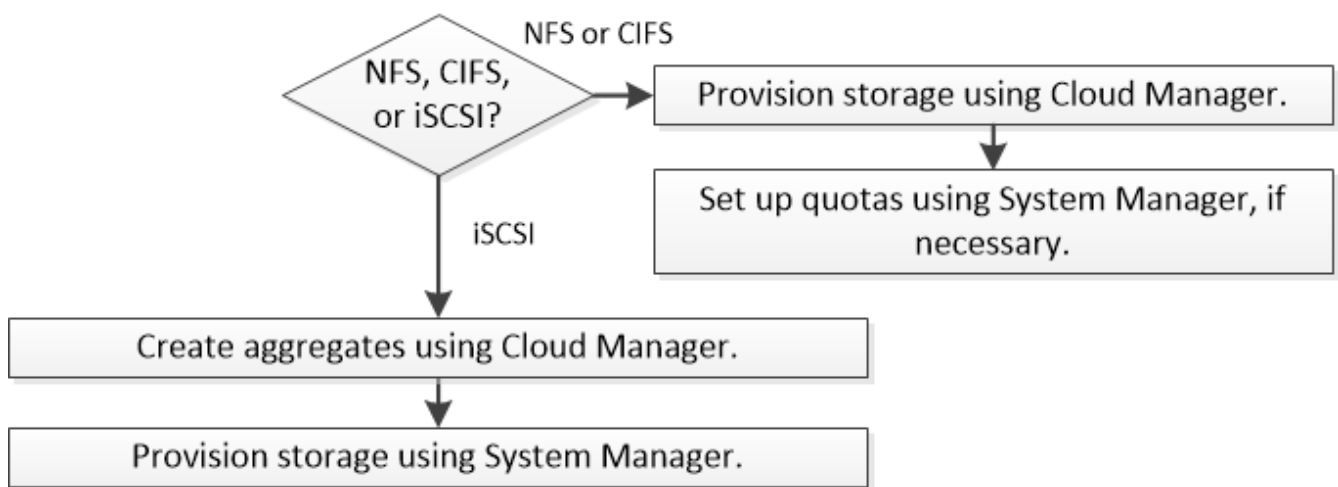
6. Provisioning storage

6.1. Provisioning storage

You can provision additional NFS and CIFS storage for your Cloud Volumes ONTAP systems from Cloud Manager by managing volumes and aggregates. If you need to create iSCSI storage, you should do so from System Manager.



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.



6.1.1. Provisioning volumes

If you need more storage after you launch a Cloud Volumes ONTAP system, you can provision new NFS and CIFS volumes from Cloud Manager.

Before you begin

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

Steps

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

Action	Steps
Create a new volume and let Cloud Manager choose the containing aggregate	Click Add New Volume .

Action	Steps
Create a new volume on a specific aggregate	<ol style="list-style-type: none"> Click the menu icon, and then click Advanced > Advanced allocation. Click the menu for an aggregate. Click Create volume.

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

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

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

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

Field	Description
DNS Primary and Secondary IP Address	<p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.</p>
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.

Field	Description
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

- On the Usage Profile, Disk Type, and Tiering Policy page, choose whether you want to enable storage efficiency features, choose a disk type, and edit the S3 tiering policy, if needed.

For help, refer to the following:

- [Understanding volume usage profiles](#)
- [Choosing an AWS disk type](#)
- [Choosing an Azure disk type](#)
- [Data tiering overview](#)

- Click **Go**.

Result

Cloud Volumes ONTAP provisions the volume.

After you finish

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

If you want to apply quotas to volumes, you must use System Manager or the CLI. Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

6.1.2. Provisioning volumes on the second node in an HA configuration

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

Steps

- On the Working Environments page, double-click the name of the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
- Click the menu icon and then click **Advanced > Advanced allocation**.
- Click **Add Aggregate** and then create the aggregate.
- For Home Node, choose the second node in the HA pair.

5. After Cloud Manager creates the aggregate, select it and then click **Create volume**.
6. Enter details for the new volume, and then click **Create**.

After you finish

You can create additional volumes on this aggregate if required.



When you mount the volume to clients, you must use the floating IP address of the node on which the volume resides.

6.1.3. Creating aggregates

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

Steps

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

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

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

6.1.4. Provisioning iSCSI LUNs

If you want to create iSCSI LUNs, you need to do so from System Manager.

Before you begin

- The Host Utilities must be installed and set up on the hosts that will connect to the LUN.
- You must have recorded the iSCSI initiator name from the host. You need to supply this name when you create an igroup for the LUN.
- Before you create volumes in System Manager, you must ensure that you have an aggregate with sufficient space. You need to create aggregates in Cloud Manager. For details, see [Creating aggregates](#).

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. [Log in to System Manager](#).
2. Click **Storage** > **LUNs**.
3. Click **Create** and follow the prompts to create the LUN.
4. Connect to the LUN from your hosts.

For instructions, see the [Host Utilities documentation](#) for your operating system.

6.2. Tiering cold data to low-cost object storage

You can reduce storage costs in AWS and Azure by combining an SSD or HDD performance tier for "hot" data with an object storage capacity tier for "cold" data. For a high-level overview, see [Data tiering overview](#).

To set up data tiering, you simply need to do the following:

[A diagram that shows the workflow for enabling tiering: choose a supported configuration, ensure that connectivity is available between tiers, and then choose a tiering policy when creating, modifying, or replicating a volume.]



What's not required for data tiering

- You do not need to install a feature license to enable data tiering.
- You do not need to create the capacity tier (either an S3 bucket or an Azure Blob container). Cloud Manager does that for you.

6.2.1. Configurations that support data tiering

You can enable data tiering when using specific configurations and features:

- Data tiering is supported with Cloud Volumes ONTAP Standard, Premium, and BYOL, starting with version 9.2 in AWS and version 9.4 in Microsoft Azure.



Data tiering is not supported in Azure with the DS3_v2 virtual machine type.

- In AWS, the performance tier can be General Purpose SSDs, Provisioned IOPS SSDs, or Throughput Optimized HDDs.
- In Azure, the performance tier can be either Premium SSD managed disks or Standard HDD managed disks.
- Data tiering is supported with AWS-managed encryption and Azure-managed encryption.
- Thin provisioning must be enabled on volumes.

6.2.2. Requirements for tiering data in AWS

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?](#).

6.2.3. Requirements for tiering data in Microsoft Azure

You do not need to set up a connection between the performance tier and the capacity tier as long as Cloud Manager has the required permissions. Cloud Manager enables a VNet service endpoint for you if the Cloud Manager policy has the appropriate permission:

"Microsoft.Network/virtualNetworks/subnets/write",

That permission is included in the latest Cloud Manager policy. For details about providing permissions, see [Granting Azure permissions](#).



If your network configuration uses route tables, then Cloud Manager also requires the following permission: Microsoft.Network/routeTables/join/action

6.2.4. Tiering data on read-write volumes

Cloud Volumes ONTAP can tier cold 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 the Snapshot Only policy or the Auto policy.

For a description of these policies, see [Data tiering overview](#).

Example

[Screenshot that shows the icon to enable tiering to object storage.]

Cloud Manager creates a new aggregate for the volume if a data tiering-enabled aggregate does not already exist.



If you prefer to create aggregates yourself, you can enable data tiering on aggregates when you create them.

6.2.5. Tiering data on 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 Working Environments 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

[Screenshot that shows the S3 tiering option when replicating a volume.]

For help with replicating data, see [Replicating data to and from the cloud](#).

6.2.6. Changing the tiering level

When you enable data tiering, Cloud Volumes ONTAP tiers cold data to the S3 *Standard* storage class in AWS or to the *hot* storage tier in Azure. After you deploy Cloud Volumes ONTAP, you can reduce your storage costs by changing the tiering level for cold data that has not 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 tiering level.

About this task

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

In AWS, you can change the tiering level so cold data moves to the *Standard-Infrequent Access* storage class or to the *One Zone-Infrequent Access* storage class after 30 days of inactivity.

In Azure, you can change the tiering level so cold data moves to the *cool* storage tier after 30 days of inactivity.

For more information about how tiering levels work, see [Data tiering overview](#).

Steps

1. From the working environment, click the menu icon and then click **Tiering Level**.
2. Choose the tiering level and then click **Save**.

6.3. Managing existing storage

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

6.3.1. Managing existing volumes


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



Steps

1. On the Working Environments 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)	<ol style="list-style-type: none">Select a volume, and then click Edit.Modify the volume's Snapshot policy, NFS access control list, or share permissions, and then click Update.
Clone a volume	<ol style="list-style-type: none">Select a volume, and then click Clone.Modify the clone name as needed, and then click Clone. <p>This process creates a FlexClone volume. A FlexClone volume is a writable, point-in-time copy that is space-efficient because it uses a small amount of space for metadata, and then only consumes additional space as data is changed or added.</p> <p>To learn more about FlexClone volumes, see the ONTAP 9 Logical Storage Management Guide.</p>
Restore data from a Snapshot copy to a new volume	<ol style="list-style-type: none">Select a volume, and then click Restore from Snapshot copy.Select a Snapshot copy, enter a name for the new volume, and then click Restore.
Create a Snapshot copy on demand	<ol style="list-style-type: none">Select a volume, and then click Create a Snapshot copy.Change the name, if needed, and then click Create.
Get the NFS mount command	<ol style="list-style-type: none">Select a volume, and then click Mount Command.Click Copy.
Change the underlying disk type	<ol style="list-style-type: none">Select a volume, and then click Change Disk Type & Tiering Policy.Select the disk type, and then click Change. <div><p>Cloud Manager moves the volume to an existing aggregate that uses the selected disk type or it creates a new aggregate for the volume.</p></div>

Task	Action
Change the tiering policy	<ol style="list-style-type: none"> Select a volume, and then click Change Disk Type & Tiering Policy. Click Edit Policy. Select a different policy and click Change. <div>  <p>Cloud Manager moves the volume to an existing aggregate that uses the selected disk type with tiering, or it creates a new aggregate for the volume.</p> </div>
Enable or disable sync to S3 for a volume	<p>Select a volume and then click Sync to S3 or Delete Sync Relationship.</p> <div>  <p>The sync to S3 feature must be enabled before you can use these options. For instructions, see Syncing data to AWS S3</p> </div>
Delete a volume	<ol style="list-style-type: none"> Select a volume, and then click Delete. Click Delete again to confirm.

6.3.2. Managing existing aggregates

If you want to manage existing aggregates yourself, you can add disks to aggregates, view information about aggregates, and delete them.

Before you begin

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

About this task

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

Steps

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

Task	Action
View information about an aggregate	Select an aggregate and click Info .

Task	Action
Create a volume on a specific aggregate	Select an aggregate and click Create volume .
Add disks to an aggregate	<ol style="list-style-type: none"> Select an aggregate and click Add AWS disks or Add Azure disks. Select the number of disks that you want to add and click Add.
Delete an aggregate	<ol style="list-style-type: none"> Select an aggregate that does not contain any volumes and click Delete. Click Delete again to confirm.

6.3.3. Modifying the CIFS server

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

Steps

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

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

- Click **Save**.

Result

Cloud Volumes ONTAP updates the CIFS server with the changes.

6.3.4. Moving a volume to avoid capacity issues

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

Steps

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

Identifying how to correct capacity issues

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

Steps

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

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

2. Identify one or more volumes to move out of the aggregate:
 - a. In the working environment, click the menu icon, and then click **Advanced** > **Advanced allocation**.
 - b. Select the aggregate, and then click **Info**.
 - c. Expand the list of volumes.

[Screen shot: Shows the list of volumes in an aggregate in the aggregate information dialog box.]

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

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

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

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

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

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

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

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

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

Moving volumes to another system to avoid capacity issues

You can move one or more volumes to another Cloud Volumes ONTAP system to avoid capacity issues. You might need to do this if the system reached its disk limit.

About this task

You can follow the steps in this task to correct the following Action Required message:

Moving a volume is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you because the system has reached the disk limit.

Steps

1. Identify a Cloud Volumes ONTAP system that has available capacity, or deploy a new system.
2. Drag and drop the source working environment on the target working environment to perform a one-time data replication of the volume.

For details, see [Replicating data between systems](#).

3. Go to the Replication Status page, and then break the SnapMirror relationship to convert the replicated volume from a data protection volume to a read/write volume.

For details, see [Managing data replication schedules and relationships](#).

4. Configure the volume for data access.

For information about configuring a destination volume for data access, see the [ONTAP 9 Volume Disaster Recovery Express Guide](#).

5. Delete the original volume.

For details, see [Managing existing volumes](#).

Moving volumes to another aggregate to avoid capacity issues

You can move one or more volumes to another aggregate to avoid capacity issues.

About this task

You can follow the steps in this task to correct the following Action Required message:

Moving two or more volumes is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you.

Steps

1. Verify whether an existing aggregate has available capacity for the volumes that you need to move:
 - a. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
 - b. Select each aggregate, click **Info**, and then view the available capacity (aggregate capacity minus used aggregate capacity).

[Screen shot: Shows the total aggregate capacity and used aggregate capacity available in the aggregate information dialog box.]

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](#).

6.4. Provisioning NFS volumes from the Volume View

6.4.1. Changing to the Volume View

Cloud Manager provides two management views: the Storage System View for managing storage systems across a hybrid cloud and the Volume View for creating volumes in AWS without having to manage storage systems. You can switch between these views, but those instances should be rare because a single view should meet your needs.

For more information about the Volume View, see [Simplified storage management using the Volume View](#).

Steps

1. In the upper right of the Cloud Manager console, click the menu, and then click **View Selection**.
2. On the View Selection page, select **Storage System View**, and then click **Switch**.

Result

Cloud Manager switches to the Volume View.

6.4.2. Creating and mounting NFS volumes

You can use Cloud Manager to create NFS volumes that provide enterprise-class features on top of AWS storage.

Creating NFS volumes

You can create a volume attached to a single AWS instance or to an instance that is mirrored to another instance to provide high availability.

Steps

1. In the Volumes tab, click **Create New Volume**.
2. On the Create New Volume page, select a volume type:

Option	Description
Create Volume	Creates a volume attached to a single AWS instance.
Create HA volume	Creates a volume attached to a single AWS instance and mirrored to another instance to provide high availability in case of failures. Click the Info icon to see additional details about the instances required for an HA volume.

3. If you chose Create Volume, specify details for your first volume, and then click **Create**.

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

Field	Description
Size	<p>The maximum size for the volume depends on the capacity available in existing storage systems.</p> <p>Thin provisioning is automatically enabled on the volume, which enables you to create a volume that is bigger than the physical storage currently available to it. Instead of preallocating storage space, space is allocated to each volume as data is written.</p>

Field	Description
AWS Disk Type	<p>You should choose the disk that meets your requirements for both performance and cost.</p> <ul style="list-style-type: none"> • General Purpose SSD disks balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS. • Throughput Optimized HDD disks are for frequently accessed workloads that require fast and consistent throughput at a lower price. • Cold HDD disks are meant for backups, or infrequently accessed data, because the performance is very low. Like Throughput Optimized HDD disks, performance is defined in terms of throughput. <p>For more details, refer to AWS Documentation: EBS Volume Types.</p>

The following image shows the Create Volume page filled out:

[Screen shot: Shows the Create New Volume page filled out.]

4. If you chose Create HA volume, specify details for the volume, and then click **Create**.

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

Field	Description
Size	<p>The maximum size for the volume depends on the capacity available in existing storage systems.</p> <p>Thin provisioning is automatically enabled on the volume, which enables you to create a volume that is bigger than the physical storage currently available to it. Instead of preallocating storage space, space is allocated to each volume as data is written.</p>
AWS Disk Type	<p>You should choose the disk that meets your requirements for both performance and cost.</p> <ul style="list-style-type: none"> • General Purpose SSD disks balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS. • Throughput Optimized HDD disks are for frequently accessed workloads that require fast and consistent throughput. <p>For more details, refer to AWS Documentation: EBS Volume Types.</p>
Location	<p>You should choose a VPC that includes three subnets in three separate Availability Zones.</p>
Nodes and Mediator	<p>If possible, Cloud Manager chooses separate Availability Zones for each instance because it is the supported and optimal configuration.</p>
Floating IP	<p>The IP addresses must be outside of the CIDR block for all VPCs in the region.</p>

Field	Description
Route Table	<p>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 HA pair.</p> <p>For more details, refer to AWS Documentation: Route Tables.</p>

The following image shows the Nodes and Mediator page. Each instance is in a separate Availability Zone.

[Screen shot: Shows AWS networking selections for the two Cloud Volumes ONTAP nodes and the mediator. Each instance is in a separate Availability Zone and subnet.]

Result

Cloud Manager creates the volume on an existing system or on a new system. If a new system is required, creating the volume can take approximately 25 minutes.

Mounting volumes to Linux hosts

After you create a volume, you should mount it to your hosts so that they can access the volume.

Steps

1. In the Volumes tab, place your mouse cursor over the volume, select the menu icon, and then click **Mount**.
2. Click **Copy**.
3. On your Linux hosts, modify the copied text by changing the destination directory, and then enter the command to mount the volume.

6.4.3. Managing NFS volumes

You can manage NFS volumes by cloning them, managing data access, changing the underlying disk type, and more.

Cloning volumes

If you need an instantaneous copy of your data without using a lot of disk space, you can create a clone of an existing volume.

About this task

The cloned 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.

Steps

1. In the Volumes tab, place your mouse cursor over the volume, select the menu icon, and then click **Clone**.
2. Modify the name of the cloned volume, if needed, and then click **Clone**.

Result

Cloud Manager creates a new volume that is a clone of an existing volume.

Managing data access to volumes

When you create a volume, Cloud Manager makes the volume available to all EC2 instances in the VPC in which the volume was created. You can modify this default value if you need to restrict data access to the volume.

Steps

1. In the Volumes tab, place your mouse cursor over the volume, select the menu icon, and then click **Manage Access**.
2. Modify the volume access list, and then click **Save**.

Changing the underlying AWS disk for a volume

You can change the underlying AWS disk that a volume uses to provide storage. For example, if higher performance is needed, you can change from a Throughput Optimized HDD to a General Purpose SSD.

Steps

1. In the Volumes tab, place your mouse cursor over the volume, select the menu icon, and then click **Change Disk**.
2. Select the AWS disk type and click **Change**.

Result

Cloud Manager moves the volume to an existing aggregate that uses the selected disk type or it creates a new aggregate for the volume.

Viewing and modifying AWS resources

When you create a new volume, Cloud Manager allocates the AWS instances and EBS storage required for that volume. If required, you can view details about AWS instances and EBS storage, change instance types, and turn instances off and on.

Steps

1. Click **AWS Resources**.

The list of AWS instances displays. You can view details such as instance type, AWS location, and the volumes attached to the instance.

2. If required, select the menu icon next to the Status column, and then choose one of the available actions:

[Screen shot that shows the available actions on the AWS Resources page in the Volume View.]

Deleting volumes

You can delete volumes that you no longer need.

Steps

1. In the Volumes tab, place your mouse cursor over the volume, select the menu icon, and then click **Delete**.
2. Click **Delete** to confirm that you want to delete the volume.

7. Managing data across a hybrid cloud

7.1. Discovering and managing ONTAP clusters

Cloud Manager can discover the ONTAP clusters in your on-premises environment, in a NetApp Private Storage configuration, and in the IBM Cloud. Discovering these clusters enables you to easily replicate data across your hybrid cloud environment directly from Cloud Manager.

7.1.1. Discovering ONTAP clusters

Discovering an ONTAP cluster in Cloud Manager enables you to provision storage and replicate data across your hybrid cloud.

Before you begin

You must have the cluster management IP address and the password for the admin user account to add the cluster to Cloud Manager.

Cloud Manager discovers ONTAP clusters using HTTPS. If you use custom firewall policies, they must meet the following requirements:

- The Cloud Manager host must allow outbound HTTPS access through port 443.

If Cloud Manager is in AWS, all outbound communication is allowed by the predefined security group.

- The ONTAP cluster must allow inbound HTTPS access through port 443.

The default "mgmt" firewall policy allows inbound HTTPS access from all IP addresses. If you modified this default policy, or if you created your own firewall policy, you must associate the HTTPS protocol with that policy and enable access from the Cloud Manager host.

Steps

1. On the Working Environments page, click **Add Working Environment**.
2. Under **Discover**, select one of the icons to discover an ONTAP cluster.

The following icon enables you to discover an on-premises cluster or a NetApp Private Storage configuration:

[Shows the ONTAP icon for discovering an on-premises ONTAP cluster.]

The following icon enables you to discover ONTAP in the IBM Cloud:

[Shows the ONTAP icon for discovering ONTAP in the IBM Cloud.]

3. On the **ONTAP Cluster Details** page, enter the cluster management IP address and the password for the admin user account.

If you selected the first icon, you must also choose the working environment type: either an on-premises cluster or a NetApp Private Storage configuration.

4. On the Details page, enter a name and description for the working environment, and then click **Go**.

Result

Cloud Manager discovers the cluster. You can now create volumes, replicate data to and from the cluster, and launch OnCommand System Manager to perform advanced tasks.

7.1.2. Provisioning volumes on ONTAP clusters

Cloud Manager enables you to provision NFS and CIFS volumes on ONTAP clusters.

Before you begin

NFS or CIFS must be set up on the cluster. You can set up NFS and CIFS using System Manager or the CLI.

About this task

You can create volumes on existing aggregates. You cannot create new aggregates from Cloud Manager.

Steps

1. On the Working Environments page, double-click the name of the ONTAP cluster on which you want to provision volumes.
2. Click **Add New Volume**.
3. On the Create New Volume page, enter details for the volume, and then click **Create**.

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.
Usage Profile	Usage profiles define the NetApp storage efficiency features that are enabled for a volume.

Field	Description
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.

7.2. Replicating data to and from the cloud

You can replicate data between working environments by choosing a one-time data replication for data transfer, or a recurring schedule for disaster recovery or long-term retention.

Cloud Manager simplifies data replication between volumes on separate systems using SnapMirror and SnapVault technologies. You simply need to identify the source volume and the destination volume, and then choose a replication policy and schedule. Cloud Manager purchases the required disks, configures relationships, applies the replication policy, and then initiates the baseline transfer between volumes.



The baseline transfer includes a full copy of the source data. Subsequent transfers contain differential copies of the source data.

7.2.1. Choosing a replication policy

A replication policy defines how the storage system replicates data from a source volume to a destination volume. You must choose a replication policy when you set up data replication in Cloud Manager.

What replication policies do

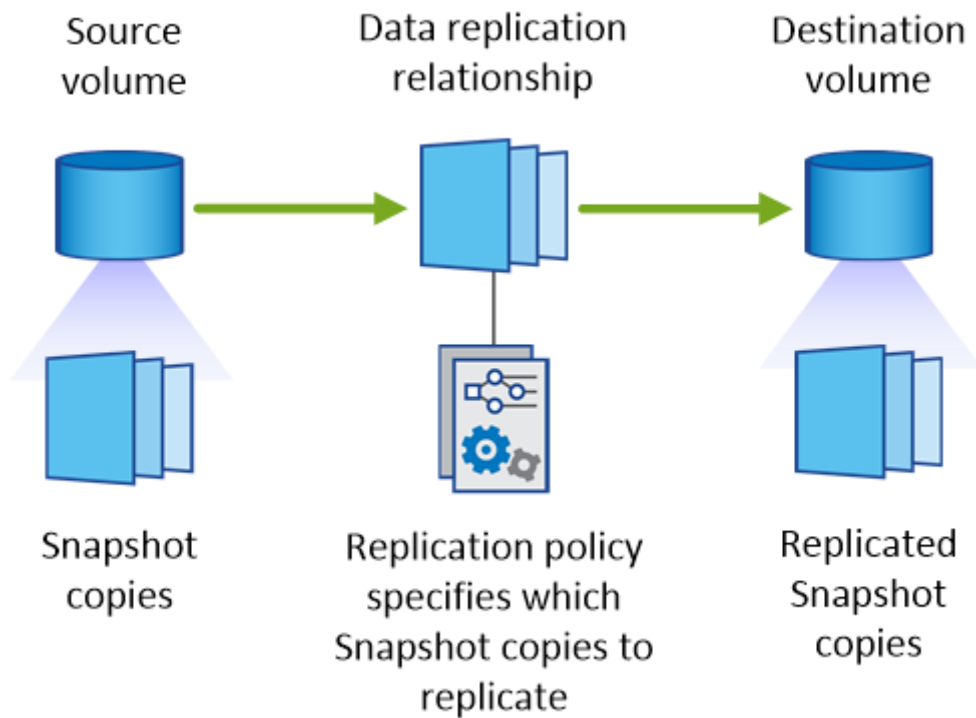
The ONTAP operating system automatically creates backups called Snapshot copies. A Snapshot copy is a read-only image of a volume that captures the state of the file system at a point in time.

When you replicate data between systems, you replicate Snapshot copies from a source volume to a destination volume. A replication policy specifies which Snapshot copies to replicate from the source volume to the destination volume.



Replication policies are also referred to as *protection* policies because they are powered by SnapMirror and SnapVault technologies, which provide disaster recovery protection and disk-to-disk backup and recovery.

The following image shows the relationship between Snapshot copies and replication policies:



Types of replication policies

There are three types of replication policies:

- A *Mirror* policy replicates newly created Snapshot copies to a destination volume.

You can use these Snapshot copies to protect the source volume in preparation for disaster recovery or for one-time data replication. You can activate the destination volume for data access at any time.

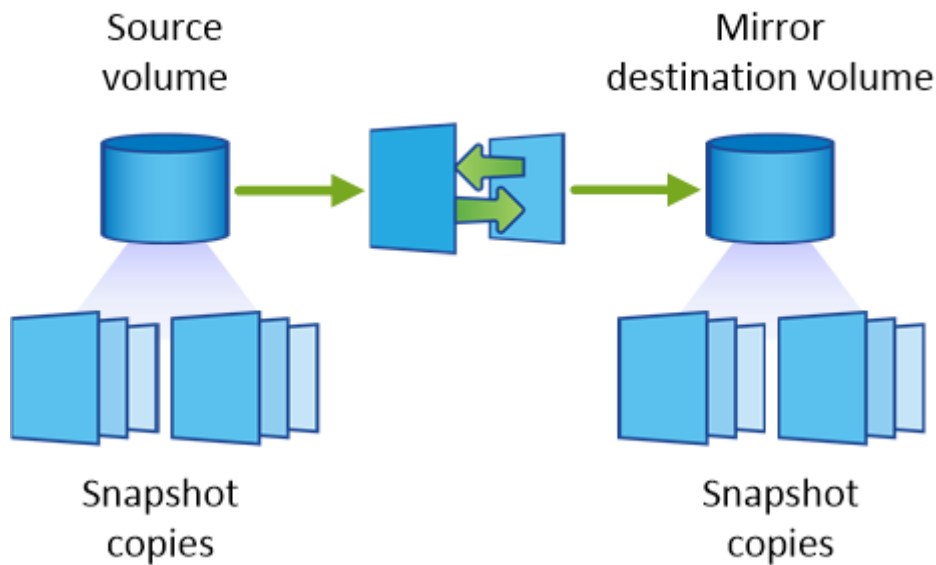
- A *Backup* policy replicates specific Snapshot copies to a destination volume and typically retains them for a longer period of time than you would on the source volume.

You can restore data from these Snapshot copies when data is corrupted or lost, and retain them for standards compliance and other governance-related purposes.

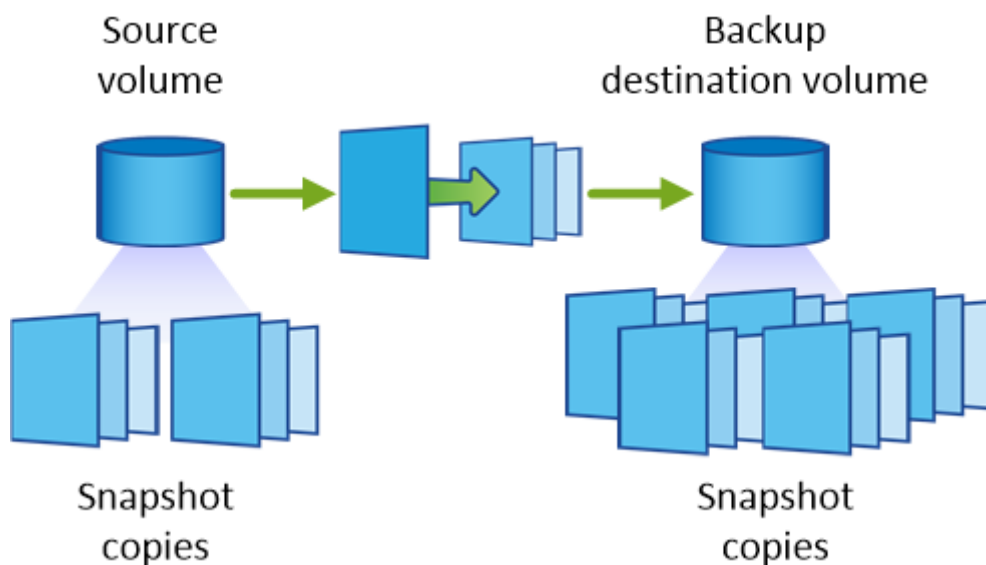
- A *Mirror and Backup* policy provides both disaster recovery and long-term retention.

Each system includes a default Mirror and Backup policy, which works well for many situations. If you find that you need custom policies, you can create your own using System Manager.

The following images show the difference between the Mirror and Backup policies. A Mirror policy mirrors the Snapshot copies available on the source volume.



A Backup policy typically retains Snapshot copies longer than they are retained on the source volume:



How Backup policies work

Unlike Mirror policies, Backup (SnapVault) policies replicate specific Snapshot copies to a destination volume. It is important to understand how Backup policies work if you want to use your own policies instead of the default policies.

Understanding the relationship between Snapshot copy labels and Backup policies

A Snapshot policy defines how the system creates Snapshot copies of volumes. The policy specifies when to create the Snapshot copies, how many copies to retain, and how to label them. For example, a system might create one Snapshot copy every day at 12:10 a.m., retain the two most recent copies, and label them "daily".

A Backup policy includes rules that specify which labeled Snapshot copies to replicate to a destination volume and how many copies to retain. The labels defined in a Backup policy must match one or more labels defined in a Snapshot policy. Otherwise, the system cannot replicate any Snapshot copies.

For example, a Backup policy that includes the labels "daily" and "weekly" results in replication of Snapshot copies that include only those labels. No other Snapshot copies are replicated, as shown in the following image:

Default policies and custom policies

The default Snapshot policy creates hourly, daily, and weekly Snapshot copies, retaining six hourly, two daily, and two weekly Snapshot copies.

You can easily use a default Backup policy with the default Snapshot policy. The default Backup policies replicate daily and weekly Snapshot copies, retaining seven daily and 52 weekly Snapshot copies.

If you create custom policies, the labels defined by those policies must match. You can create custom policies using System Manager.

7.2.2. Data replication requirements

Before you can replicate data, you should confirm that specific requirements are met for both Cloud Volumes ONTAP systems and ONTAP clusters.

Version requirements

You should verify that the source and destination volumes are running compatible ONTAP versions before replicating data. For details, see the [Data Protection Power Guide](#).

Requirements specific to Cloud Volumes ONTAP

- The instance's security group must include the required inbound and outbound rules: specifically, rules for ICMP and ports 10000, 11104, and 11105.

These rules are included in the predefined security group.

- To replicate data between two Cloud Volumes ONTAP systems in different subnets, the subnets must be routed together (this is the default setting).
- To replicate data between a Cloud Volumes ONTAP system in AWS and a system in Azure, you must have a VPN connection between the AWS VPC and the Azure VNet.

Requirements specific to ONTAP clusters

- An active SnapMirror license must be installed.
- If the cluster is on your premises, you should have a connection from your corporate network to AWS or Azure, which is typically a VPN connection.
- ONTAP clusters must meet additional subnet, port, firewall, and cluster requirements.

For details, see the Cluster and SVM Peering Express Guide for your version of ONTAP.

7.2.3. Replicating data between systems

You can replicate data between Cloud Volumes ONTAP systems and ONTAP clusters by choosing a one-time data replication, which can help you move data to and from the cloud, or a recurring schedule, which can help with disaster recovery or long-term retention.

About this task

Cloud Manager supports simple, fanout, and cascade data protection configurations:

- In a simple configuration, replication occurs from volume A to volume B.
- In a fanout configuration, replication occurs from volume A to multiple destinations.
- In a cascade configuration, replication occurs from volume A to volume B and from volume B to volume C.

You can configure fanout and cascade configurations in Cloud Manager by setting up multiple data replications between systems. For example, by replicating a volume from system A to system B and then by replicating the same volume from system B to system C.

Steps

1. On the Working Environments 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:

[Screen shot: Shows a working environment being placed on top of another working environment to start the data replication process.]

2. If the Source and Destination Peering Setup pages appear, select all of the intercluster LIFs for the cluster peer relationship.

The intercluster network should be configured so that cluster peers have *pair-wise full-mesh connectivity*, which means that each pair of clusters in a cluster peer relationship has connectivity among all of their intercluster LIFs.

These pages appear if an ONTAP cluster that has multiple LIFs is the source or destination.

3. On the Source Volume Selection page, select the volume that you want to replicate.
4. On the Destination Volume Name and Tiering page, specify the destination volume name, choose an underlying disk type, change any of the advanced options, and then click **Continue**.

If the destination is an ONTAP cluster, you must also specify the destination SVM and aggregate.

5. On the Max Transfer Rate page, specify the maximum rate (in megabytes per second) at which data can be transferred.
6. On the Replication Policy page, choose one of the default policies or click **Additional Policies**, and then select one of the advanced policies.

For help, see [Choosing a replication policy](#).

If you choose a custom backup (SnapVault) policy, the labels associated with the policy must

match the labels of the Snapshot copies on the source volume. For more information, see [How backup policies work](#).

7. On the Schedule page, choose a one-time copy or a recurring schedule.

Several default schedules are available. If you want a different schedule, you must create a new schedule on the *destination* cluster using System Manager.

8. On the Review page, review your selections, and then click **Go**.

Result

Cloud Manager starts the data replication process. You can view details about the replication in the Replication Status page.

7.2.4. Managing data replication schedules and relationships

After you set up data replication between two systems, you can manage the data replication schedule and relationship from Cloud Manager.

Steps

1. On the Working Environments page, view the replication status for all assigned working environments in the tenant or for a specific working environment:

Option	Action
All assigned working environments in the tenant	Click Replication Status from the navigation bar. [Screen shot: Shows the Replication Status tab.]
A specific working environment	Select the working environment, and then click Replication Status. [Screen shot: Shows the Replication Status icon available from the working environments page.]

2. Review the status of the data replication relationships to verify that they are healthy.




If the Status of a relationship is idle and the Mirror State is uninitialized, you must initialize the relationship from the destination system for the data replication to occur according to the defined schedule. You can initialize the relationship by using System Manager or the command-line interface (CLI). These states can appear when the destination system fails and then comes back online.

3. Select the menu icon next to the source volume, and then choose one of the available actions.

[Screen shot: Shows the list of actions available from the Replication Status page.]

The following table describes the available actions:

Action	Description
Break	<p>Breaks the relationship between the source and destination volumes, and activates the destination volume for data access.</p> <p>This option is typically used when the source volume cannot serve data due to events such as data corruption, accidental deletion, or an offline state.</p> <p>For information about configuring a destination volume for data access and reactivating a source volume, see the ONTAP 9 Volume Disaster Recovery Express Guide.</p>
Resync	<p>Reestablishes a broken relationship between volumes and resumes data replication according to the defined schedule.</p> <div>  <p>When you resynchronize the volumes, the contents on the destination volume are overwritten by the contents on the source volume.</p> </div> <p>To perform a reverse resync, which resynchronizes the data from the destination volume to the source volume, see the ONTAP 9 Volume Disaster Recovery Express Guide.</p>
Reverse Resync	<p>Reverses the roles of the source and destination volumes. Contents from the original source volume are overwritten by contents of the destination volume. This is helpful when you want to reactivate a source volume that went offline.</p> <p>Any data written to the original source volume between the last data replication and the time that the source volume was disabled is not preserved.</p>
Edit Schedule	Enables you to choose a different schedule for data replication.
Policy Info	Shows you the protection policy assigned to the data replication relationship.
Edit Max Transfer Rate	Enables you to edit the maximum rate (in kilobytes per second) at which data can be transferred.
Delete	Deletes the data protection relationship between the source and destination volumes, which means that data replication no longer occurs between the volumes. This action does not activate the destination volume for data access. This action also deletes the cluster peer relationship and the storage virtual machine (SVM) peer relationship, if there are no other data protection relationships between the systems.

Result

After you select an action, Cloud Manager updates the relationship or schedule.

7.3. Syncing data to AWS S3

You can sync data from ONTAP volumes to an AWS S3 bucket by integrating a working environment with [NetApp Cloud Sync](#). You can then use the synced data as a secondary copy or for data processing using AWS services like EMR and Redshift.

7.3.1. How the sync to S3 feature works

You can integrate a working environment with the Cloud Sync service at any time. When you integrate a working environment, the Cloud Sync service syncs data from the selected volumes to a single S3 bucket. The integration works with Cloud Volumes ONTAP working environments, as well as ONTAP clusters that are on-premises or part of a NetApp Private Storage (NPS) configuration.

To sync the data, the service launches a data broker instance in your VPC. Cloud Sync uses one data broker per working environment to sync data from volumes to an S3 bucket. After the initial sync, the service syncs any changed data once per day at midnight.

[Screen shot: Shows a conceptual image of volumes from a working environment being synced to an S3 bucket by a data broker.]

If you want to perform advanced Cloud Sync actions, go directly to the Cloud Sync service. From there, you can perform actions such as syncing from S3 to an NFS server, choosing different S3 buckets for volumes, and modifying schedules.



The sync to S3 feature is available for Cloud Manager Admins and Tenant Admins only.

14-day free trial

If you are a new Cloud Sync user, your first 14 days are free. After the free trial ends, you must pay for each *sync relationship* at an hourly rate or by purchasing licenses. Each volume that you sync to an S3 bucket is considered a sync relationship. You can set up both payment options directly from Cloud Sync in the License Settings page.

How to get help

Use the following options for any support related to the Cloud Manager sync to S3 feature or for Cloud Sync in general:

- General product feedback: ng-cloudsync-contact@netapp.com
- Technical Support options:
 - NetApp Cloud Sync Communities
 - In-product chat (lower-right corner of Cloud Manager)

7.3.2. Integrating a working environment with the Cloud Sync service

If you want to sync volumes to AWS S3 directly from Cloud Manager, then you must integrate the working environment with the Cloud Sync service.

► https://www.youtube.com/watch?v=3hOtLs70_xE (YouTube video)

Steps

1. Open a working environment and click **Sync to S3**.
2. Click **Sync** and follow the prompts to sync your data to S3.



You cannot sync data protection volumes to S3. The volumes must be writable.

7.3.3. Managing volume sync relationships

After you integrate a working environment with the Cloud Sync service, you can sync additional volumes, stop syncing a volume, and remove the integration with Cloud Sync.

Steps

1. On the Working Environments page, double-click the working environment on which you want to manage sync relationships.
2. If you want to enable or disable sync to S3 for a volume, select the volume and then click **Sync to S3** or **Delete Sync Relationship**.
3. If you want to delete all sync relationships for a working environment, click the **Sync to S3** tab and then click **Delete Sync**.

This action does not delete synced data from the S3 bucket. If the data broker is not being used in any other sync relationships, then the Cloud Sync service deletes the data broker.

8. Administering Cloud Volumes ONTAP

8.1. Connecting to Cloud Volumes ONTAP

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using OnCommand System Manager or the command line interface.

8.1.1. Connecting to OnCommand System Manager

You might need to perform some Cloud Volumes ONTAP tasks from OnCommand System Manager, which is a browser-based management tool that runs on the Cloud Volumes ONTAP system. For example, you need to use System Manager if you want to create LUNs.

Before you begin

The computer from which you are accessing Cloud Manager must have a network connection to Cloud Volumes ONTAP. For example, you might need to log in to Cloud Manager from a jump host in AWS or Azure.



When deployed in multiple AWS Availability Zones, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

Steps

1. From the Working Environments page, double-click the Cloud Volumes ONTAP system that you want to manage with System Manager.
2. Click the menu icon, and then click **Advanced** > **System Manager**.
3. Click **Launch**.

System Manager loads in a new browser tab.

4. At the login screen, enter **admin** in the User Name field, enter the password that you specified when you created the working environment, and then click **Sign In**.

Result

The System Manager console loads. You can now use it to manage Cloud Volumes ONTAP.

8.1.2. Connecting to the Cloud Volumes ONTAP CLI

The Cloud Volumes ONTAP CLI enables you to execute all administrative commands and is a good choice for advanced tasks or if you are more comfortable using the CLI. You can connect to the CLI using Secure Shell (SSH).

Before you begin

The host from which you use SSH to connect to Cloud Volumes ONTAP must have a network connection to Cloud Volumes ONTAP. For example, you might need to use SSH from a jump host in

AWS or Azure.



When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

Steps

1. In Cloud Manager, identify the IP address of the cluster management interface:
 - a. On the Working Environments 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:

[Screen shot: Shows the destination admin@192.168.11.5 on port 22.]

3. At the login prompt, enter the password for the admin account.

Example

```
Password: *****  
COT2::>
```

8.2. Updating Cloud Volumes ONTAP software

Cloud Manager includes several options that you can use to upgrade to the current Cloud Volumes ONTAP release or to downgrade Cloud Volumes ONTAP to an earlier release. You should prepare Cloud Volumes ONTAP systems before you upgrade or downgrade the software.

8.2.1. Overview

Cloud Manager displays a notification in Cloud Volumes ONTAP working environments when a new version of Cloud Volumes ONTAP is available:

[Screen shot: Shows the New version available notification which displays in the Working Environments page after you select a working environment.]

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.



Upgrades of HA pairs are nondisruptive—HA pairs continue to serve data during the upgrade process.

Cloud Manager might upgrade the HA mediator as part of this process.

Advanced options for software updates

Cloud Manager also provides the following advanced options for updating Cloud Volumes ONTAP software:

- Software updates using an image on an external URL

This option is helpful if Cloud Manager cannot access the S3 bucket to upgrade the software, if you were provided with a patch, or if you want to downgrade the software to a specific version.

- Software updates using the alternate image on the system

You can use this option to downgrade to the previous version by making the alternate software image the default image. This option is not available for HA pairs.

Transitioning Cloud Volumes ONTAP to an earlier release in the same release family (for example, 9.3 to 9.2) is referred to as a downgrade. You can downgrade without assistance when downgrading new or test clusters, but you should contact technical support if you want to downgrade a production cluster.

8.2.2. Preparing to update Cloud Volumes ONTAP software

Before performing an upgrade or downgrade, you must verify that your systems are ready and make any required configuration changes.

Suspending SnapMirror transfers

If a Cloud Volumes ONTAP system has active SnapMirror relationships, it is best to suspend transfers before you update the Cloud Volumes ONTAP software. Suspending the transfers prevents SnapMirror failures. You must suspend the transfers from the destination system.

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. [Log in to System Manager](#) from the destination system.
2. Click **Protection > Relationships**.
3. Select the relationship and click **Operations > Quiesce**.

Verifying that aggregates are online

Aggregates for Cloud Volumes ONTAP must be online before you update the software. Aggregates should be online in most configurations, but if they are not, then you should bring them online.

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
2. Select an aggregate, click **Info**, and then verify that the state is online.

[Screen shot: Shows the State field when you view information for an aggregate.]

3. If the aggregate is offline, use System Manager to bring the aggregate online:
 - a. [Log in to System Manager](#).
 - b. Click **Storage > Aggregates & Disks > Aggregates**.
 - c. Select the aggregate, and then click **More Actions > Status > Online**.

8.2.3. Upgrading Cloud Volumes ONTAP to the latest version

You can upgrade to the latest version of Cloud Volumes ONTAP directly from Cloud Manager. Cloud Manager notifies you when a new version is available.

Before you begin

Cloud Manager operations such as volume or aggregate creation must not be in progress for the Cloud Volumes ONTAP system.

About this task

The upgrade process takes up to 25 minutes for a single Cloud Volumes ONTAP system and up to 90 minutes for an HA pair. Upgrades of HA pairs are nondisruptive. HA pairs continue to serve data during the upgrade process.

Steps

1. Click **Working Environments**.
2. Select a working environment.

A notification appears in the right pane if a new version is available:

[Screen shot: Shows the New version available notification which displays in the Working Environments page after you select a working environment.]

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.

8.2.4. Upgrading or downgrading Cloud Volumes ONTAP by using an HTTP or FTP server

You can place the Cloud Volumes ONTAP software image on an HTTP or FTP server and then initiate the software update from Cloud Manager. You might use this option if Cloud Manager cannot access the S3 bucket to upgrade the software or if you want to downgrade the software.

About this task

This upgrade or downgrade process takes up to 25 minutes for a single Cloud Volumes ONTAP system and up to 90 minutes for an HA pair. Upgrades and downgrades of HA pairs are nondisruptive. HA pairs continue to serve data during the process.

Steps

1. Set up an HTTP server or FTP server that can host the Cloud Volumes ONTAP software image.
2. If you have a VPN connection to the VPC, you can place the Cloud Volumes ONTAP software image on an HTTP server or FTP server in your own network. Otherwise, you must place the file on an HTTP server or FTP server in AWS.
3. If you use your own security group for Cloud Volumes ONTAP, ensure that the outbound rules allow HTTP or FTP connections so Cloud Volumes ONTAP can access the software image.



The predefined Cloud Volumes ONTAP security group allows outbound HTTP and FTP connections by default.

4. Obtain the software image from [NetApp Downloads: Software](#).
5. Copy the software image to the directory on the HTTP or FTP server from which the file will be served.
6. From the working environment in Cloud Manager, click the menu icon, and then click **Advanced > Update Cloud Volumes ONTAP**.
7. On the update software page, choose **Select an image available from a URL**, enter the URL, and then click **Change Image**.
8. Click **Proceed** to confirm.

Result

Cloud Manager starts the software update. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

8.2.5. Downgrading Cloud Volumes ONTAP by using a local image

Each Cloud Volumes ONTAP system can hold two software images: the current image that is running, and an alternate image that you can boot. Cloud Manager can change the alternate image to be the default image. You can use this option to downgrade to the previous version of Cloud Volumes ONTAP, if you are experiencing issues with the current image.

About this task

This downgrade process is available for single Cloud Volumes ONTAP systems only. It is not available for HA pairs. The process takes the Cloud Volumes ONTAP system offline for up to 25 minutes.

Steps

1. From the working environment, click the menu icon, and then click **Advanced > Update Cloud Volumes ONTAP**.
2. On the update software page, select the alternate image, and then click **Change Image**.
3. Click **Proceed** to confirm.

Result

Cloud Manager starts the software update. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

8.3. Modifying Cloud Volumes ONTAP systems

You might need to change the configuration of Cloud Volumes ONTAP instances as your storage needs change. For example, you can change between pay-as-you-go configurations, change the instance or VM type, and move to an alternate subscription.

8.3.1. Installing license files on Cloud Volumes ONTAP BYOL systems

If Cloud Manager cannot obtain a BYOL license file from NetApp, you can obtain the file yourself and then manually upload the file to Cloud Manager so it can install the license on the Cloud Volumes ONTAP system.

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 (either **NetApp Cloud Volumes ONTAP BYOL for AWS**, **NetApp Cloud Volumes ONTAP BYOL for Azure**, or **NetApp Cloud Volumes ONTAP BYOL HA for AWS**), enter the serial number, confirm that you have read and accepted the privacy policy, and then click **Submit**.

Example

[Screen shot: Shows an example of the NetApp License File Generator web page filled out, including a password, a product (NetApp Cloud Volumes ONTAP BYOL for AWS), and a product serial number.]

3. Choose whether you want to receive the serialnumber.NLF JSON file through email or direct download.
4. In Cloud Manager, select the Cloud Volumes ONTAP BYOL working environment.
5. In the Storage pane, click the menu icon, and then click **License**.
6. Click **Upload License File**.
7. Click **Upload** and then select the file.

Result

Cloud Manager installs the new license file on the Cloud Volumes ONTAP system.

8.3.2. Changing the instance or virtual machine type for Cloud Volumes ONTAP

You can choose from several instance or virtual machine types when you launch Cloud Volumes ONTAP in AWS or Azure. You can change the instance or virtual machine type at any time if you determine that it is undersized or oversized for your needs.

About this task

- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

For HA pairs, the change is nondisruptive. HA pairs continue to serve data.

- Changing the instance or virtual machine type affects AWS or Azure service charges.

Steps

1. From the working environment, click the menu icon, and then click **Change license or instance** for AWS or click **Change license or VM** for Azure.
2. If you are using a pay-as-you-go configuration, you can optionally choose a different license.
3. Select an instance or virtual machine type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

Result

Cloud Volumes ONTAP reboots with the new configuration.

8.3.3. Changing between pay-as-you-go configurations

After you launch pay-as-you-go Cloud Volumes ONTAP systems, you can change between the Explore, Standard, and Premium configurations at any time by modifying the license. Changing the license increases or decreases the raw capacity limit and enables you to choose from different EC2 instance types or Azure virtual machine types.

About this task

Note the following about changing between pay-as-you-go licenses:

- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

For HA pairs, the change is nondisruptive. HA pairs continue to serve data.

- Changing the instance or virtual machine type affects AWS or Azure service charges.

Steps

1. From the working environment, click the menu icon, and then click **Change license or instance** for AWS or click **Change license or VM** for Azure.
2. Select a license type and an instance type or virtual machine type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

Result

Cloud Volumes ONTAP reboots with the new license, instance type or virtual machine type, or both.

8.3.4. Moving to an alternate Cloud Volumes ONTAP configuration

If you want to move between a pay-as-you-go subscription and a BYOL subscription or between a single Cloud Volumes ONTAP system and an HA pair, you can deploy a new system and then replicate data from the existing system to the new system.

Steps

1. Create a new Cloud Volumes ONTAP working environment.

[Launching Cloud Volumes ONTAP in AWS](#)

[Launching Cloud Volumes ONTAP in Azure](#)

2. If you chose a pay-as-you-go license and the tenant does not have a NetApp Support Site account assigned to it, [manually register the systems with NetApp](#).

Support from NetApp is included with Cloud Volumes ONTAP. To activate support, you must first register the system with NetApp.

3. [Set up one-time data replication](#) between the systems for each volume that you must replicate.
4. Terminate the Cloud Volumes ONTAP system that you no longer need by [deleting the original working environment](#).

8.3.5. Modifying the storage virtual machine name

Cloud Manager automatically names the storage virtual machine (SVM) for Cloud Volumes ONTAP. You can modify the name of the SVM if you have strict naming standards. For example, you might want it to match how you name the SVMs for your ONTAP clusters.

Steps

1. From the working environment, click the menu icon, and then click **Information**.
2. Click the edit icon to the right of the SVM name.

[Screen shot: Shows the SVM Name field and the edit icon that you must click to modify the SVM name.]

3. In the Modify SVM Name dialog box, modify the SVM name, and then click **Save**.

8.3.6. Changing the password for Cloud Volumes ONTAP

Cloud Volumes ONTAP includes a cluster admin account. You can change the password for this account from Cloud Manager, if needed.



You should not change the password for the admin account through System Manager or the CLI. The password will not be reflected in Cloud Manager. As a result, Cloud Manager cannot monitor the instance properly.

Steps

1. From the working environment, click the menu icon, and then click **Advanced > Set password**.
2. Enter the new password twice and then click **Save**.

The new password must be different than one of the last six passwords that you used.

8.3.7. Changing the network MTU for c4.4xlarge and c4.8xlarge instances

By default, Cloud Volumes ONTAP is configured to use 9,000 MTU (also called jumbo frames) when you choose the c4.4xlarge instance or the c4.8xlarge instance in AWS. You can change the network MTU to 1,500 bytes if that is more appropriate for your network configuration.

About this task

A network maximum transmission unit (MTU) of 9,000 bytes can provide the highest maximum network throughput possible for specific configurations.

9,000 MTU is a good choice if clients in the same VPC communicate with the Cloud Volumes ONTAP system and some or all of those clients also support 9,000 MTU. If traffic leaves the VPC, packet fragmentation can occur, which degrades performance.

A network MTU of 1,500 bytes is a good choice if clients or systems outside of the VPC communicate with the Cloud Volumes ONTAP system.

Steps

1. From the working environment, click the menu icon and then click **Advanced > Network Utilization**.
2. Select **Standard** or **Jumbo Frames**.
3. Click **Change**.

8.3.8. Changing route tables associated with HA pairs

You can modify the route tables that include routes to the floating IP addresses for an HA pair. You might do this if new NFS or CIFS clients need to access the HA pair.

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.

8.4. Managing the state of Cloud Volumes ONTAP

You can stop and start Cloud Volumes ONTAP from Cloud Manager to manage your cloud compute costs.

8.4.1. 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

This task schedules automatic shutdowns of both nodes in an HA pair.

Steps

1. From the working environment, click the clock icon:

[Screen shot: Shows the icon that loads the automatic shutdown page.]

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.

[Screen shot: Shows a shutdown schedule that shuts down Cloud Volumes ONTAP every weekend at 12:00 AM for 48 hours.]

3. Click **Save**.

Result

Cloud Manager saves the schedule. The clock icon changes to indicate that a schedule is set: [Screen shot: Shows the automatic shutdown icon after a schedule is defined.]

8.4.2. 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.

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.

[Screen shot: Shows the icon to turn off a Cloud Volumes ONTAP system.]

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.

8.5. Monitoring AWS storage and compute costs

You can view the cost associated with running Cloud Volumes ONTAP in AWS. The monthly cost consists of the compute purchased from AWS to run Cloud Volumes ONTAP and the disks purchased from AWS for Cloud Volumes ONTAP use.

Before you begin

The AWS payer account must meet specific billing and cost requirements and your Cloud Manager account must be associated with the AWS cost S3 bucket. For instructions, see [Setting up AWS billing and cost management for Cloud Manager](#).

About this task

Cloud Manager updates the storage and compute costs every 12 hours. You should refer to AWS for final cost details.

Step

1. On the Working Environments 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 storage costs savings, if you enabled NetApp's efficiency features on volumes. If the cost information is not available, verify that the Cloud Manager Admin met the prerequisites listed earlier.

The following image shows an example of the AWS costs per month:

[Screen shot: Shows the costs per month for a Cloud Volumes ONTAP instance.]

The following image shows an example of storage cost savings:

[Screen shot: Shows the storage cost savings for a Cloud Volumes ONTAP instance.]

8.6. 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 your Cloud Manager system became unusable and you launched a new system, but you could not restore all Cloud Volumes ONTAP systems from a recent Cloud Manager backup.

Before you begin

You must know the password for the Cloud Volumes ONTAP admin user account.

Steps

1. On the Working Environments page, click **Add Working Environment**.
2. Under Discover, select **Cloud Volumes ONTAP**.

[Screen shot: Shows the Cloud Volumes ONTAP icon for creating or discovering an instance.]

3. On the Region page, choose the region where the instances are running, and then select the instances.
4. 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 tenant.

8.7. Deleting a Cloud Volumes ONTAP working environment

It is best to delete Cloud Volumes ONTAP systems from Cloud Manager, rather than from AWS or Azure. For example, if you terminate a licensed Cloud Volumes ONTAP instance from AWS, you cannot use the license key for another instance. You must delete the working environment from Cloud Manager to release the license.

About this task

When you delete a working environment, Cloud Manager terminates instances, deletes disks, and

snapshots.



Cloud Volumes ONTAP instances have termination protection enabled to help prevent accidental termination from AWS. However, if you do terminate a Cloud Volumes ONTAP instance from AWS, you must go to the AWS CloudFormation console and delete the instance's stack. The stack name is the name of the working environment.

Steps

1. From the working environment, click menu icon and then click **Delete**.
2. Type the name of the working environment and then click **Delete**.

It can take up to 5 minutes to delete the working environment.

9. Administering Cloud Manager

9.1. Updating Cloud Manager

You can update Cloud Manager to the latest version or with a patch that NetApp personnel shared with you.

9.1.1. Enabling automatic updates

Cloud Manager can automatically update itself to the latest maintenance or minor release whenever a new version is available. This ensures that you are running the latest version.

About this task

Cloud Manager automatically updates at 12:00 midnight if no operations are running.

Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **Settings**.
2. Select the checkbox under Automatic Cloud Manager Updates and then click **Save**.

9.1.2. Updating Cloud Manager to the latest version

You should enable automatic updates to Cloud Manager, but you can always do a manual update directly from the web console. Cloud Manager obtains the software update from a NetApp-owned S3 bucket in AWS.

Before you begin

You should have reviewed [what is new in the release](#) to identify new requirements and changes in support.

About this task

The software update takes a few minutes. Cloud Manager will not be available during the update.

Steps

1. Check whether a new version is available by looking at the lower-right corner of the console:

[Screen shot: Shows the New version available link that is available from the lower-right hand corner of the Cloud Manager web console.]

2. If a new version is available, click **Timeline** to determine whether any tasks are in progress.

If any tasks are in progress, wait for them to finish before you proceed to the next step.

3. In the lower-right of the console, click **New version available**.
4. On the Cloud Manager Software Update page, click **Update** next to the version that you want.
5. Complete the confirmation dialog box, and then click **OK**:

- a. Keep the option to download a backup because you can use it to restore your Cloud Manager configuration, if necessary.
 - b. Read the terms and conditions, and then select the **I read and approve the terms and conditions (EULA)** check box.
6. When prompted, save the Cloud Manager backup.

Result

Cloud Manager starts the update process. You can log in to the console after a few minutes.

9.1.3. Updating Cloud Manager with a patch

If NetApp shared a patch with you, you can update Cloud Manager with the supplied patch directly from the Cloud Manager web console.

About this task

The patch update typically takes a few minutes. Cloud Manager will not be available during the update.

Steps

1. In the upper-right hand corner of the Cloud Manager console, click the task drop-down list, and then select **Update**.
2. Click the link to update Cloud Manager with the supplied patch.

[Screen shot: Shows the link to update Cloud Manager with a patch.]

3. Complete the confirmation dialog box and then click **OK**:
 - a. Keep the option to download a backup enabled because you can use it to restore your Cloud Manager configuration, if necessary.
 - b. Read the terms and conditions and then select the **I read and approve the terms and conditions (EULA)** check box.
4. Select the patch that you were provided.
5. When prompted, save the Cloud Manager backup.

Result

Cloud Manager applies the patch. You can log in to the console after a few minutes.

9.2. Backing up and restoring Cloud Manager

Cloud Manager enables you to back up and restore its database to protect your configuration and troubleshoot issues.

9.2.1. Backing up Cloud Manager

It is a good practice to back up the Cloud Manager database on a periodic basis. If you experience problems, you can restore Cloud Manager from a previous backup.

Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **Tools**.
2. Click **Backup**.

[Screen shot: Shows the Backup button in the Tools page.]

3. When prompted, save the backup file to a secure location so that you can retrieve it when needed.

9.2.2. Restoring Cloud Manager from a backup

Restoring Cloud Manager from a backup replaces existing data with the data from the backup.

Steps

1. In the upper-right hand corner of the Cloud Manager console, click the task drop-down list, and then select **Tools**.
2. Click **Restore**.
3. Click **OK** to confirm.
4. Select the backup.

Result

Cloud Manager restores the database from the backup file.

9.3. Removing Cloud Volumes ONTAP working environments

The Cloud Manager 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 tenant
- Rediscover it from another Cloud Manager system
- Rediscover it if you had problems during the initial discovery

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then 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 Working Environments page at any time.

9.4. Editing user accounts

You can modify user accounts in Cloud Manager by changing the cloud permissions associated with the account, enabling and disabling the notification report, and by changing the S3 cost bucket for detailed billing reports.

About this task

Password and user information must be changed in [NetApp Cloud Central](#).

Steps

1. In the upper-right corner of the Cloud Manager console, click the user icon, and then select **View Users**.
2. Select the menu icon at the end of the row and click **Edit User**.

[Screen shot: Shows the menu to edit a user account. The menu is located next to the user name.]

3. In the User Settings page, modify the user account.

9.5. Configuring Cloud Manager to use a proxy server

When you first deploy Cloud Manager, it prompts you to enter a proxy server if the system does not have internet access. You can also manually enter and modify the proxy from Cloud Manager's settings.

About this task

If your corporate policies dictate that you use a proxy server for all HTTP communication to the internet, then you must configure Cloud Manager to use that proxy server. The proxy server can be in the cloud or in your network.

When you configure Cloud Manager to use a proxy server, Cloud Manager, Cloud Volumes ONTAP, and the HA mediator all use the proxy server.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then select **Settings**.
2. Under HTTP Proxy, enter the server using the syntax `http://address:port`, specify a user name and password if basic authentication is required for the server, and then click **Save**.



Cloud Manager does not support passwords that include the @ character.

Result

After you specify the proxy server, new Cloud Volumes ONTAP systems are automatically configured to use the proxy server when sending AutoSupport messages. If you do not specify the proxy server before users create Cloud Volumes ONTAP systems, then they must use System Manager to manually set the proxy server in the AutoSupport options for each system.

9.6. Managing encryption settings for Cloud Volumes ONTAP

You might need to periodically manage Cloud Manager encryption settings to ensure that Cloud Volumes ONTAP systems in AWS can communicate with key managers.



Data-at-rest encryption provided by Cloud Volumes ONTAP is no longer supported when launching new Cloud Volumes ONTAP systems in AWS. Existing systems that use this feature are still supported. See [What's new in Cloud Manager](#) for more details.

9.6.1. Renewing the Cloud Manager intermediate CA certificate

You must renew the Cloud Manager certificate before it expires; otherwise, Cloud Manager cannot sign client certificates for Cloud Volumes ONTAP.

About this task

If you renew the Cloud Manager intermediate CA certificate, Cloud Manager uses the renewed certificate to generate client certificates for *new* Cloud Volumes ONTAP systems. You can renew client certificates for *existing* Cloud Volumes ONTAP systems from the working environment.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then click **Encryption Setup**.
2. In the Intermediate CA tab, click **Renew Intermediate CA**.
3. Click **Generate CSR**.
4. Use the CSR to submit a certificate request to a CA.

The intermediate CA certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.

5. Copy the contents of the signed certificate and paste it in the Cloud Manager certificate field.
6. Click **Install Cloud Manager Certificate**.

9.6.2. Managing available key managers and CA certificates

You can modify the key managers and key manager CA certificates that Cloud Manager users can use with their Cloud Volumes ONTAP systems. For example, you can add a new key manager that is available in your environment and you can add a new CA certificate, if a previous certificate expired.

About this task

The changes that you make from the Encryption Setup page affect only new Cloud Volumes ONTAP systems. Changes to existing Cloud Volumes ONTAP systems must be made from the working environment.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then click **Encryption Setup**.
2. Click **Key Manager**.
3. Manage your key managers as necessary:

Action	Steps
Change the KMIP port for communicating with key managers	<p>Modify the port and then click Save.</p> <p>The port change affects only new Cloud Volumes ONTAP systems.</p> <p>To change the port for an existing Cloud Volumes ONTAP system, connect to the CLI and then run the security key-manager setup command.</p>
Add a new key manager	<p>Click Add, enter details about the key manager, and then click Add again.</p> <p>This action does not add the key manager to existing Cloud Volumes ONTAP systems. You must add the key manager from the working environment, if necessary.</p>
Edit the details for a key manager	<p>Select the menu icon next to the key manager, click Edit, modify the details, and then click Save.</p> <p>Any changes affect only new Cloud Volumes ONTAP systems that will use this key manager. To apply this change to existing Cloud Volumes ONTAP systems, go to the working environment, remove the key manager, and then add it back.</p>
Delete an existing key manager	<p>Select the menu icon next to the key manager, click Delete, and then click Delete again.</p> <p>If you delete a key manager, you cannot configure Cloud Volumes ONTAP systems to use it. Existing systems that are using this key manager can continue to use it.</p>

4. Manage the key managers' CA certificates as necessary:

Action	Steps
Add a new certificate	Click Add , paste the certificate, and then click Add again.
View a certificate	Select the menu icon next to the key manager and click View .
Delete a certificate	<p>Select the menu icon next to the certificate, click Delete, and then click Delete again.</p> <p>If you delete a certificate, you cannot configure Cloud Volumes ONTAP systems to use it. Existing systems that are using the certificate can continue to use it.</p>

9.7. Renewing the Cloud Manager HTTPS certificate

You should renew the Cloud Manager HTTPS certificate before it expires to ensure secure access to the Cloud Manager web console. If you do not renew the certificate before it expires, a warning appears when users access the web console using HTTPS.

Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **HTTPS Setup**.

Details about the Cloud Manager certificate displays, including the expiration date.

2. Click **Renew HTTPS Certificate** and follow the steps to generate a CSR or install your own CA-signed certificate.

Result

Cloud Manager uses the new CA-signed certificate to provide secure HTTPS access.

9.8. Uninstalling Cloud Manager

Cloud Manager includes an uninstallation script that you can use to uninstall the software to troubleshoot issues or to permanently remove the software from the host.

Steps

1. If you are going to reinstall Cloud Manager, back up the database before you uninstall the software:
 - a. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then select **Tools**.
 - b. Click **Backup** and save the backup file to your local machine.
2. From the Linux host, run the uninstallation script:

`/opt/application/netapp/cloudmanager/bin/uninstall.sh [silent]`

silent runs the script without prompting you for confirmation.

10. Reference

10.1. Frequently asked questions: Integrating Cloud Manager with NetApp Cloud Central

When upgrading to Cloud Manager 3.5, NetApp will choose specific Cloud Manager systems to integrate with NetApp Cloud Central, if they are not already integrated. This FAQ can answer questions that you might have about the process.

10.1.1. What is NetApp Cloud Central?

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

10.1.2. Why is NetApp integrating my Cloud Manager system with Cloud Central?

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

10.1.3. What happens during the integration process?

NetApp migrates all local user accounts in your Cloud Manager system to the centralized user authentication available in Cloud Central.

10.1.4. How does centralized user authentication work?

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

10.1.5. Do I need to sign up for a Cloud Central user account?

NetApp will create a Cloud Central user account for you when we integrate your Cloud Manager system with Cloud Central. You simply need to reset your password to complete the registration process.

10.1.6. What if I already have a Cloud Central user account?

If the email address that you use to log in to Cloud Manager matches the email address for a Cloud Central user account, then you can log right in to your Cloud Manager system.

10.1.7. What if my Cloud Manager system has multiple user accounts?

NetApp migrates all local user accounts to Cloud Central user accounts. Every user needs to reset his or her password.

10.1.8. What if I have a user account that uses the same email address across multiple Cloud Manager systems?

You just need to reset your password once and then you can use the same Cloud Central user account to log in to each Cloud Manager system.

10.1.9. What if my local user account uses an invalid email address?

Resetting your password requires a valid email address. Contact us through the chat icon that is available in the lower right of the Cloud Manager interface.

10.1.10. What if I have automation scripts for Cloud Manager APIs?

All APIs are backwards compatible. You will need to update scripts that use passwords, if you change your password when you reset it.

10.1.11. What if my Cloud Manager system uses LDAP?

If your system uses LDAP, NetApp cannot automatically integrate the system with Cloud Central. You need to manually perform the following steps:

1. Deploy a new Cloud Manager system from [NetApp Cloud Central](#).
2. [Set up LDAP with the new system](#).
3. [Discover existing Cloud Volumes ONTAP systems](#) from the new Cloud Manager system.
4. Delete the old Cloud Manager system.

10.1.12. Does it matter where I installed my Cloud Manager system?

No. NetApp will integrate systems with Cloud Central no matter where they reside, whether that's in AWS, Azure, or on your premises.



The only exception is the AWS Commercial Cloud Services Environment.

10.2. Supported regions

Cloud Manager and Cloud Volumes ONTAP are supported in a number of AWS regions and Microsoft Azure regions.

10.2.1. Supported AWS regions

You can deploy Cloud Manager and Cloud Volumes ONTAP in the following AWS regions.

Asia Pacific

- Mumbai
- Seoul
- Singapore
- Sydney
- Tokyo

EU

- Frankfurt
- Ireland
- London
- Paris

North America

- Canada (Central)
- GovCloud (US)
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)

South America

- Sao Paulo

10.2.2. Supported Azure regions

You can deploy Cloud Manager and Cloud Volumes ONTAP in the following Azure regions.

Asia Pacific

- Australia East
- Australia Southeast
- Central India
- East Asia
- Japan East
- Japan West
- Korea Central
- Korea South

- South India
- Southeast Asia
- West India

EU

- Germany Central
- Germany Northeast
- North Europe
- UK South
- UK West
- West Europe

North America

- Canada Central
- Canada East
- Central US
- East US
- East US 2
- North Central US
- South Central US
- US Gov Arizona
- US Gov Texas
- US Gov Virginia
- West US
- West US 2
- West Central US

South America

- Brazil South

10.3. Security group rules for AWS

Cloud Manager creates AWS security groups that include the inbound and outbound rules that Cloud Manager 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.

10.3.1. Rules for Cloud Manager

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

Inbound rules for Cloud Manager

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

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Cloud Manager host
HTTP	80	Provides HTTP access from client web browsers to the Cloud Manager web console
HTTPS	443	Provides HTTPS access from client web browsers to the Cloud Manager web console

Outbound rules for Cloud Manager

The predefined security group for Cloud Manager 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 Manager 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 Cloud Manager.



The source IP address is the Cloud Manager host.

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

10.3.2. Rules for Cloud Volumes ONTAP

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

Inbound rules for Cloud Volumes ONTAP

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

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the System Manager web console using the IP address of the cluster management LIF
HTTPS	443	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS

Protocol	Port	Purpose
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
UDP	635	NFS mount
UDP	2049	NFS server daemon
UDP	4045	NFS lock daemon
UDP	4046	Network status monitor for NFS
UDP	4049	NFS rquotad protocol

Outbound rules for Cloud Volumes ONTAP

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

Basic outbound rules

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

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

Advanced outbound rules

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



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

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

Service	Protocol	Port	Source	Destination	Purpose
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
	TCP	3000	Node management LIF	HA mediator	ZAPI calls (Cloud Volumes ONTAP HA only)
	ICMP	1	Node management LIF	HA mediator	Keep alive (Cloud Volumes ONTAP HA only)
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	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
Syslog	UDP	514	Node management LIF	Syslog server	Syslog forward messages

10.3.3. 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 Cloud Manager

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.

Service	Protocol	Port	Destination	Purpose
API	HTTP S	443	AWS API services	Assist with storage failover
API	UDP	53	AWS API services	Assist with storage failover



Rather than open these two ports, you can use a private endpoint instead.

10.3.4. Rules for the HA mediator internal security group

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

Inbound rules

The predefined security group includes the following inbound rules.

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

Outbound rules

The predefined security group includes the following outbound rules.

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

10.4. Security group rules for Azure

Cloud Manager creates Azure security groups that include the inbound and outbound rules that Cloud Manager 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.

10.4.1. Rules for Cloud Manager

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

Inbound rules for Cloud Manager

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

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Cloud Manager host
HTTP	80	Provides HTTP access from client web browsers to the Cloud Manager web console
HTTPS	443	Provides HTTPS access from client web browsers to the Cloud Manager web console

Outbound rules for Cloud Manager

The predefined security group for Cloud Manager 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 Manager 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 Cloud Manager.



The source IP address is the Cloud Manager host.

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

10.4.2. Rules for Cloud Volumes ONTAP

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

Inbound rules for Cloud Volumes ONTAP

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

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the System Manager web console using the IP address of the cluster management LIF
HTTPS	443	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
UDP	635	NFS mount
UDP	2049	NFS server daemon
UDP	4045	NFS lock daemon
UDP	4046	Network status monitor for NFS
UDP	4049	NFS rquotad protocol

Outbound rules for Cloud Volumes ONTAP

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

Basic outbound rules

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

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

Advanced outbound rules

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



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

Service	Protocol	Port	Source	Destination	Purpose
Active Directory	TCP	88	Node management LIF	Active Directory forest	Kerberos V authentication
	UDP	137	Node management LIF	Active Directory forest	NetBIOS name service
	UDP	138	Node management LIF	Active Directory forest	NetBIOS datagram service
	TCP	139	Node management LIF	Active Directory forest	NetBIOS service session
	TCP	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)	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	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)
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup

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

10.5. Cloud Manager REST APIs

Cloud Manager includes REST APIs that enable software developers to automate the management of NetApp storage in the cloud. There is an API for every action that is available from the user interface.

Cloud Manager provides interactive API documentation using the Swagger interface. A link to the API documentation is available in the lower-right corner of the console:

[Shows the API documentation link that is available from the lower-right hand corner of the Cloud Manager web console.]

You can also find an overview, examples, and an API reference in the [OnCommand Cloud Manager API Developer Guide](#).

10.6. AWS and Azure permissions for Cloud Manager

Cloud Manager requires permissions to perform actions in AWS and Azure on your behalf. These permissions are included in [the policies provided by NetApp](#). You might want to understand what Cloud Manager does with these permissions.

10.6.1. What Cloud Manager does with AWS permissions

Cloud Manager uses an AWS account to make API calls to several AWS services, including EC2, S3, CloudFormation, IAM, the Security Token Service (STS), and the Key Management Service (KMS).

Actions	Purpose
"ec2:StartInstances", "ec2:StopInstances", "ec2:DescribeInstances", "ec2:DescribeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModifyInstanceAttribute",	Launches a Cloud Volumes ONTAP instance and stops, starts, and monitors the instance.
"ec2:DescribeInstanceAttribute",	Verifies that enhanced networking is enabled for supported instance types.
"ec2:DescribeRouteTables", "ec2:DescribeImages",	Launches a Cloud Volumes ONTAP HA configuration.
"ec2:CreateTags",	Tags every resource that Cloud Manager creates with the "WorkingEnvironment" and "WorkingEnvironmentId" tags. Cloud Manager uses these tags for maintenance and cost allocation.
"ec2:CreateVolume", "ec2:DescribeVolumes", "ec2:ModifyVolumeAttribute", "ec2:AttachVolume", "ec2>DeleteVolume", "ec2:DetachVolume",	Manages the EBS volumes that Cloud Volumes ONTAP uses as back-end storage.
"ec2:CreateSecurityGroup", "ec2>DeleteSecurityGroup", "ec2:DescribeSecurityGroups", "ec2:RevokeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",	Creates predefined security groups for Cloud Volumes ONTAP.

Actions	Purpose
"ec2:CreateNetworkInterface", "ec2:DescribeNetworkInterfaces", "ec2:DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute",	Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet.
"ec2:DescribeSubnets", "ec2:DescribeVpcs",	Gets the list of destination subnets and security groups, which is needed when creating a new working environment for Cloud Volumes ONTAP.
"ec2:DescribeDhcpOptions",	Determines DNS servers and the default domain name when launching Cloud Volumes ONTAP instances.
"ec2:CreateSnapshot", "ec2:DeleteSnapshot", "ec2:DescribeSnapshots",	Takes snapshots of EBS volumes during initial setup and whenever a Cloud Volumes ONTAP instance is stopped.
"ec2:GetConsoleOutput",	Captures the Cloud Volumes ONTAP console, which is attached to AutoSupport messages.
"ec2:DescribeKeyPairs",	Obtains the list of available key pairs when launching instances.
"ec2:DescribeRegions",	Gets a list of available AWS regions.
"ec2:DeleteTags", "ec2:DescribeTags",	Manages tags for resources associated with Cloud Volumes ONTAP instances.
"cloudformation:CreateStack", "cloudformation>DeleteStack", "cloudformation:DescribeStacks", "cloudformation:DescribeStackEvents", "cloudformation:ValidateTemplate",	Launches Cloud Volumes ONTAP instances.
"iam:PassRole", "iam:CreateRole", "iam:DeleteRole", "iam:PutRolePolicy", "iam:CreateInstanceProfile", "iam:DeleteRolePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "iam:DeleteInstanceProfile",	Launches a Cloud Volumes ONTAP HA configuration.
"iam:ListInstanceProfiles", "sts:DecodeAuthorizationMessage", "ec2:AssociateIamInstanceProfile", "ec2:DescribeIamInstanceProfileAssociations", "ec2:DisassociateIamInstanceProfile",	Manages instance profiles for Cloud Volumes ONTAP instances.
"s3:GetObject", "s3:ListBucket"	Obtains AWS cost data for Cloud Volumes ONTAP.


Actions	Purpose
"s3:GetBucketTagging", "s3:GetBucketLocation", "s3:ListAllMyBuckets",	Obtains information about AWS S3 buckets so Cloud Manager can integrate with the NetApp Data Fabric Cloud Sync service.
"s3:CreateBucket", "s3:DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions",	Manages the S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier.
"kms:List*", "kms:Describe*"	Obtains information about keys from the AWS Key Management Service.

10.6.2. What Cloud Manager does with Azure permissions

The Cloud Manager Azure policy includes the permissions that Cloud Manager needs to deploy and manage Cloud Volumes ONTAP in Azure.

Actions	Purpose
"Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read", "Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", "Microsoft.Compute/virtualMachines/vmSizes/read", "Microsoft.Compute/virtualMachines/write",	Creates Cloud Volumes ONTAP and stops, starts, deletes, and obtains the status of the system.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Enables Cloud Volumes ONTAP deployment from a VHD.

Actions	Purpose
"Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checknameavailability/read", "Microsoft.Storage/operations/read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/storageAccounts/read", "Microsoft.Storage/storageAccounts/regeneratekey/action", "Microsoft.Storage/storageAccounts/write"	Manages Azure storage accounts and disks, and attaches the disks to Cloud Volumes ONTAP.
"Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action",	Creates and manages network interfaces for Cloud Volumes ONTAP in the target subnet.
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action",	Creates predefined network security groups for Cloud Volumes ONTAP.
"Microsoft.Resources/subscriptions/locations/read", "Microsoft.Network/locations/operationResults/read", "Microsoft.Network/locations/operations/read", "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", "Microsoft.Network/virtualNetworks/virtualMachines/read", "Microsoft.Network/virtualNetworks/subnets/join/action",	Gets network information about regions, the target VNet and subnet, and adds Cloud Volumes ONTAP to VNets.

Actions	Purpose
<p>"Microsoft.Network/virtualNetworks/subnets/write",</p> <div data-bbox="183 383 248 443">  </div> <p>If your network configuration uses route tables, then Cloud Manager also requires the following permission: Microsoft.Network/routeTables/join/action</p>	Enables VNet service endpoints for data tiering.
<p>"Microsoft.Resources/deployments/operations/read", "Microsoft.Resources/deployments/read", "Microsoft.Resources/deployments/write",</p>	Deploys Cloud Volumes ONTAP from a template.
<p>"Microsoft.Resources/deployments/operations/read", "Microsoft.Resources/deployments/read", "Microsoft.Resources/deployments/write", "Microsoft.Resources/resources/read", "Microsoft.Resources/subscriptions/operationresults/read", "Microsoft.Resources/subscriptions/resourceGroups/delete", "Microsoft.Resources/subscriptions/resourceGroups/read", "Microsoft.Resources/subscriptions/resourceGroups/resources/read", "Microsoft.Resources/subscriptions/resourceGroups/write",</p>	Creates and manages resource groups for Cloud Volumes ONTAP.
<p>"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/disks/beginGetAccess/action"</p>	Creates and manages Azure managed snapshots.
<p>"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",</p>	Creates and manages availability sets for Cloud Volumes ONTAP.
<p>"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read", "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write"</p>	Enables programmatic deployments from the Azure Marketplace.
<p>"Microsoft.Authorization/locks/*"</p>	Enables management of locks on Azure disks.

10.7. Default configurations

Details about how Cloud Manager and Cloud Volumes ONTAP are configured by default can help you administer the systems.

10.7.1. Default configuration for Cloud Manager on Linux

If you need to troubleshoot Cloud Manager or your Linux host, it might help to understand how Cloud Manager is configured.

- If you deployed Cloud Manager from NetApp Cloud Central (or directly from the AWS Marketplace or Azure Marketplace), note the following:
 - In AWS, the user name for the EC2 Linux instance is `ec2-user`.
 - For both AWS and Azure, the operating system for the Cloud Manager image is Red Hat Enterprise Linux 7.4 (HVM).

The operating system does not include a GUI. You must use a terminal to access the system.

- The Cloud Manager installation folder resides in the following location:

`/opt/application/netapp/cloudmanager`

- Log files are contained in the following folder:

`/opt/application/netapp/cloudmanager/log`

- The Cloud Manager service is named `occm`.
- The `occm` service is dependent on the MySQL service.

If the MySQL service is down, then the `occm` service is down too.

- Cloud Manager installs the following packages on the Linux host, if they are not already installed:
 - 7Zip
 - AWSCLI
 - Java
 - MySQL
 - Wget

10.7.2. 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.

- Cloud Volumes ONTAP is available as a single system in AWS and Microsoft Azure, and as an HA

pair in AWS.

- Cloud Manager creates one data-serving SVM when it deploys Cloud Volumes ONTAP. While you can create another data-serving SVM from System Manager or the CLI, using multiple data-serving SVMs is not supported.
- Several network interfaces are created by default:
 - A cluster management LIF
 - An intercluster LIF
 - 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 EC2 requirements. Migrating a LIF to a different port breaks the external mapping between IP addresses and network interfaces on the instance, making the LIF inaccessible.

- Cloud Volumes ONTAP sends configuration backups to Cloud Manager using HTTPS.
- When logged in to Cloud Manager, the backups are accessible from <https://ipaddress/occm/offboxconfig/>
- Cloud Manager sets a few volume attributes differently than other management tools (System Manager or the CLI, for example).

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

Attribute	Value set by Cloud Manager
Autosize mode	grow
Maximum autosize	1,000 percent <div> The Cloud Manager Admin can modify this value from the Settings page.</div>
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.

10.7.3. Boot and root data for Cloud Volumes ONTAP

In addition to the storage for user data, Cloud Manager also purchases cloud storage for boot and root data on each Cloud Volumes ONTAP system.

AWS

- One Provisioned IOPS SSD disk for Cloud Volumes ONTAP boot data, which is approximately 45 GB and 1,250 PIOPS
- One General Purpose SSD disk for Cloud Volumes ONTAP root data, which is approximately 140 GB
- One EBS snapshot for each boot disk and root disk

In an HA pair, both Cloud Volumes ONTAP nodes replicate its root disk to the partner node.

Azure

- One Premium Storage SSD disk for Cloud Volumes ONTAP boot data, which is approximately 73 GB
- One Premium Storage SSD disk for Cloud Volumes ONTAP root data, which is approximately 140 GB
- One Azure snapshot for each boot disk and root disk

Where the disks reside

Cloud Manager lays out the storage from AWS and Azure as follows:

- Boot data resides on a disk attached to the EC2 instance or Azure 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.

10.8. User roles

Each Cloud Manager user account is assigned a role that defines permissions.

Task	Cloud Manager Admin	Tenant Admin	Working Environment Admin
Manage tenants	Yes	No	No
Manage working environments	Yes	Yes, for the assigned tenant	Yes, for assigned working environments

Task	Cloud Manager Admin	Tenant Admin	Working Environment Admin
Integrate a working environment with Cloud Sync	Yes	Yes	No
View data replication status	Yes	Yes, for the assigned tenant	Yes, for assigned working environments
View the timeline	Yes	Yes	Yes
Create and delete user accounts	Yes	Yes, for the assigned tenant	No
Modify user accounts	Yes	Yes, for the assigned tenant	Yes, for their own account
Switch between the Storage System View and the Volume View	Yes	No	No
Modify settings	Yes	No	No
View and manage the Support Dashboard	Yes	No	No
Back up and restore Cloud Manager	Yes	No	No
Remove a working environment	Yes	No	No
Update Cloud Manager	Yes	No	No
Install an HTTPS certificate	Yes	No	No
Set up Active Directory	Yes	No	No
Enable the Cloud Storage Automation Report	Yes	No	No

10.9. Where to get help and find more information

You can get help and find more information about Cloud Manager and Cloud Volumes ONTAP through various resources, including videos, forums, and support.

- [Videos for Cloud Manager and Cloud Volumes ONTAP](#)

Watch videos that show you how to deploy and manage Cloud Volumes ONTAP in AWS and Azure and how to replicate data across your hybrid cloud.

- [Policies for Cloud Manager](#)

Download JSON files that include the permissions that Cloud Manager needs to perform actions in AWS and Azure.

- [Cloud Manager API Developer Guide](#)

Read an overview of the APIs, examples of how to use them, and an API reference.

- Technical reports

- [NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads](#)
- [NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads](#)

- [Cloud Volumes ONTAP 9 SVM Disaster Recovery Preparation Express Guide](#)

Describes how to quickly configure a destination SVM in preparation for disaster recovery.

- [Cloud Volumes ONTAP 9 SVM Disaster Recovery Express Guide](#)

Describes how to quickly activate a destination SVM after a disaster, and then reactivate the source SVM.

- [ONTAP 9 Documentation Center](#)

Access product documentation for ONTAP, which can help you as you use Cloud Volumes ONTAP.

- [NetApp Cloud Volumes ONTAP Support](#)

Access support resources to get help and troubleshoot issues with Cloud Volumes ONTAP.

- [NetApp Community: Hybrid Cloud](#)

Connect with peers, ask questions, exchange ideas, find resources, and share best practices.

- [NetApp Cloud Central](#)

Find information about additional NetApp products and solutions for the cloud.

- [NetApp Product Documentation](#)

Search NetApp product documentation for instructions, resources, and answers.

- [Notice for Cloud Manager 3.5](#)

Provides information about third-party copyright and licenses.

11. Earlier versions of Cloud Manager documentation

Documentation for previous releases of Cloud Manager is available in case you are not running the latest version.

- [Cloud Manager 3.4](#)
- [Cloud Manager 3.3](#)
- [Cloud Manager 3.2](#)