



# **Use Cloud Volumes ONTAP**

## **Cloud Volumes ONTAP**

NetApp  
June 01, 2022

This PDF was generated from <https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-manage-capacity-licenses.html> on June 01, 2022. Always check docs.netapp.com for the latest.

# Table of Contents

- Use Cloud Volumes ONTAP ..... 1
  - License management ..... 1
  - Volume and LUN administration ..... 10
  - Aggregate administration ..... 32
  - Storage VM administration ..... 34
  - Security and data encryption ..... 57
  - System administration ..... 70
  - System health and events ..... 92

# Use Cloud Volumes ONTAP

## License management

### Manage capacity-based licenses

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

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

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

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

### How licenses are added to the Digital Wallet

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

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

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

### View your account's capacity

View the licensed capacity and provisioned capacity by package to ensure that you have enough room for your data volumes.

### Steps

1. Click **All Services > Digital Wallet > Cloud Volumes ONTAP**.
2. With **Capacity Based Licenses** selected, view the licensed capacity and provisioned capacity for each package.



3. If needed, purchase additional licensed capacity and then add the license to your account.

### Add purchased licenses to your account

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

#### What you'll need

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

#### Steps

1. Click **All Services > Digital Wallet > Cloud Volumes ONTAP**.
2. Click **Add License**.
3. Enter the serial number for your capacity-based license or upload the license file.

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

4. Click **Add License**.

### Update a capacity-based license

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

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

#### What you'll need

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

#### Steps

1. Click **All Services > Digital Wallet > Cloud Volumes ONTAP**.
2. Click the action menu next to the license and select **Update License**.
3. Upload the license file.

4. Click **Upload License**.

### Remove a capacity-based license

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

#### Steps

1. Click **All Services > Digital Wallet > Cloud Volumes ONTAP**.
2. Click the action menu next to the license and select **Remove License**.
3. Click **Remove** to confirm.

## Manage Keystone Flex Subscriptions

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

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

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

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

### Authorize your account

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

#### Steps

1. Click **All Services > Digital Wallet**.
2. Click **Keystone Flex Subscription**.
3. If you see the **Welcome to NetApp Keystone** page, send an email to the address listed on the page.

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

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



## What's next?

Link the subscriptions that you want to use with Cloud Volumes ONTAP.

## Link a subscription

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

### Steps

1. Click **All Services > Digital Wallet**.
2. Click **Keystone Flex Subscription**.
3. For the subscription that you want to link, click **...** and select **Link**.

Subscription Number	Committed	Consumed	# of Instances	Expiration Date	
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022	...
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022	
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022	

View detail and edit  
Link

## Result

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

## Request more or less committed capacity

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

### Steps

1. Click **All Services > Digital Wallet**.
2. Click **Keystone Flex Subscription**.
3. For the subscription that you want adjust the capacity, click **...** and select **View detail and edit**.
4. Enter the requested committed capacity for one or more subscriptions.

### Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity
Extreme	0.977 TiB	0.293 TiB	<input type="text" value="Enter amount"/> TiB
Premium	0.977 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB
Performance	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
Standard	0.732 TiB	0.439 TiB	<input type="text" value="Enter amount"/> TiB
Value	0.977 TiB	 0.879 TiB	<input type="text" value="Enter amount"/> TiB
Data Tiering	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
CVO Primary	1.96 TiB	 1.76 TiB	<input type="text" value="3"/> TiB
CVO Secondary	1.02 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB

#### Additional Information

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

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

## Result

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

## Unlink a subscription

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

## Steps

1. Click **All Services > Digital Wallet**.
2. Click **Keystone Flex Subscription**.
3. For the subscription that you want to unlink, click **...** and select **Unlink**.

## Result

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

## Manage node-based licenses

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

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

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

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

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

## Manage PAYGO licenses

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

### Steps

1. Click **All Services > Digital Wallet > Cloud Volumes ONTAP**.
2. Select **Node Based Licenses** from the drop-down.
3. Click **PAYGO**.
4. View details in the table about each of your PAYGO licenses.



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



## Manage BYOL licenses

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

### Add unassigned licenses

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

#### Steps

1. Click **All Services > Digital Wallet > Cloud Volumes ONTAP**.
2. Select **Node Based Licenses** from the drop-down.
3. Click **Unassigned**.
4. Click **Add Unassigned Licenses**.
5. Enter the serial number of the license or upload the license file.

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

6. Click **Add License**.

#### Result

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

### Exchange unassigned node-based licenses

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

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

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

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

#### Steps

1. Click **All Services > Digital Wallet > Cloud Volumes ONTAP**.
2. Select **Node Based Licenses** from the drop-down.
3. Click **Unassigned**.
4. Click **Exchange License**.

BYOL (14)	Eval (2)	Unassigned (3)	PAYGO (6)	<input type="text"/> <input type="button" value="Add Unassigned Licenses"/>		
Serial Number	Type	Cloud Provider	License Expiry	Status		
012345678901234567890	Single Node	All Providers	April 20, 2022	Unassigned	Exchange License ▾	...
012345678901234567891	Single Node	 Azure	April 20, 2022	Unassigned	Exchange License ▾	...
012345678901234567892	Single Node	 AWS	January 1, 2022	Exchanged to Cloud Tiering on August 1, 2021		...

5. Select the service that you'd like to exchange the license with.
6. If you're prompted, select an additional license for the HA pair.
7. Read the legal consent and click **Agree**.

## Result

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

## Obtain a system license file

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

## Steps

1. Go to the [NetApp License File Generator](#) and log in using your NetApp Support Site credentials.
2. Enter your password, choose your product, enter the serial number, confirm that you have read and accepted the privacy policy, and then click **Submit**.

## Example

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

## Update a system license

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

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

## Steps

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

6. Click **Update License**.

## Result

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

## Manage extra capacity licenses

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

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

## Add capacity licenses

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

### Steps

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

## Update capacity licenses

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

### Steps

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

## Remove capacity licenses

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

### Steps

1. Click **All Services > Digital Wallet > Cloud Volumes ONTAP**.
2. Select **Node Based Licenses** from the drop-down.
3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.

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

### Convert an Eval license to a BYOL

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

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

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

### Steps

1. Click **All Services > Digital Wallet > Cloud Volumes ONTAP**.
2. Select **Node Based Licenses** from the drop-down.
3. Click **Eval**.
4. In the table, click **Convert to BYOL License** for a Cloud Volumes ONTAP system.
5. Enter the serial number or upload the license file.
6. Click **Convert License**.

### Result

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

## Volume and LUN administration

### Create FlexVol volumes

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

Cloud Manager provides several ways to create a new volume:

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

### Before you get started

A few notes about volume provisioning:

- When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, [use the IQN to connect to the LUN from your hosts](#).

- You can create additional LUNs from System Manager or the CLI.
- If you want to use CIFS in AWS, you must have set up DNS and Active Directory. For details, see [Networking requirements for Cloud Volumes ONTAP for AWS](#).

## Create a volume

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

### Steps

1. On the Canvas page, double-click the name of the Cloud Volumes ONTAP system on which you want to provision a FlexVol volume.
2. Create a new volume by letting Cloud Manager handle the disk allocation for you, or choose a specific aggregate for the volume.

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

#### Any aggregate

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

#### Specific aggregate

- a. Click the menu icon, and then click **Advanced > Advanced allocation**.
- b. Click the menu for an aggregate.
- c. Click **Create volume**.

3. Follow the steps in the wizard to create the volume.
  - a. **Details, Protection, and Tags:** Enter basic details about the volume and select a Snapshot policy.

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

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

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

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

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

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

## NFS

### Access control

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

### Export policy

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

## CIFS

### Permissions and users/groups

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

### DNS Primary and Secondary IP Address

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

If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.

### Active Directory Domain to join

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

### Credentials authorized to join the domain

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

### CIFS server NetBIOS name

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

### Organizational Unit

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

- To configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=corp** in this field.
- To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, enter **OU=AADDC Computers** or **OU=AADDC Users** in this field.  
[Azure Documentation: Create an Organizational Unit \(OU\) in an Azure AD Domain Services managed domain](#)
- To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=Cloud** in this field.  
[Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD](#)

### DNS Domain

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

## NTP Server

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

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

## iSCSI

### LUN

iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, [use the IQN to connect to the LUN from your hosts](#).

### Initiator group

Initiator groups (igroups) specify which hosts can access specified LUNs on the storage system

### Host initiator (IQN)

iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bus adapters (HBAs) and are identified by iSCSI qualified names (IQNs).

- c. **Disk Type:** Choose an underlying disk type for the volume based on your performance needs and cost requirements.
- [Sizing your system in AWS](#)
  - [Sizing your system in Azure](#)
  - [Sizing your system in Google Cloud](#)
- d. **Usage Profile & Tiering Policy:** Choose whether to enable or disable storage efficiency features on the volume and then select a [volume tiering policy](#).

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

### Thin provisioning

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

### Deduplication

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

### Compression

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



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

## Result

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

## Create a volume from a template

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

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



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

## Steps

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



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



The *Define Parameters* page is displayed.



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

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

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



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

7. Click **Run Template**.

### Result

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



**Creating your resources**

This process can take a few minutes.

Keep this page open to monitor progress, or you can close this page and check the [Timeline](#) later for details.

**Actions status**

	<div>Create Volume in Cloud Volumes ONTAP</div>	<div>Success</div>
	<div>Enable Cloud Backup</div>	<div>Pending</div>

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

### Create a volume on the second node in an HA configuration

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

#### Steps

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

4. For Home Node, choose the second node in the HA pair.
5. After Cloud Manager creates the aggregate, select it and then click **Create volume**.
6. Enter details for the new volume, and then click **Create**.

## Result

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



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

## After you create a volume

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

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

## Manage existing volumes


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

## Manage volumes

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

## Steps

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

Task	Action
View information about a volume	Select a volume, and then click <b>Info</b> .
Edit a volume (read-write volumes only)	<ol style="list-style-type: none"> <li>a. Select a volume, and then click <b>Edit</b>.</li> <li>b. Modify the volume's Snapshot policy, NFS protocol version, NFS access control list (export policy), or share permissions, and then click <b>Update</b>.</li> </ol> <div>  <p>If you need custom Snapshot policies, you can create them by using System Manager.</p> </div>

Task	Action
Clone a volume	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Clone</b>.</li> <li>Modify the clone name as needed, and then click <b>Clone</b>.</li> </ol> <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 <a href="#">ONTAP 9 Logical Storage Management Guide</a>.</p>
Restore data from a Snapshot copy to a new volume	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Restore from Snapshot copy</b>.</li> <li>Select a Snapshot copy, enter a name for the new volume, and then click <b>Restore</b>.</li> </ol>
Create a Snapshot copy on demand	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Create a Snapshot copy</b>.</li> <li>Change the name, if needed, and then click <b>Create</b>.</li> </ol>
Get the NFS mount command	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Mount Command</b>.</li> <li>Click <b>Copy</b>.</li> </ol>
View the target iQN for an iSCSI volume	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Target iQN</b>.</li> <li>Click <b>Copy</b>.</li> <li><a href="#">Use the IQN to connect to the LUN from your hosts</a>.</li> </ol>
Change the underlying disk type	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Change Disk Type &amp; Tiering Policy</b>.</li> <li>Select the disk type, and then click <b>Change</b>.</li> </ol> <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>
Change the tiering policy	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Change Disk Type &amp; Tiering Policy</b>.</li> <li>Click <b>Edit Policy</b>.</li> <li>Select a different policy and click <b>Change</b>.</li> </ol> <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>
Delete a volume	<ol style="list-style-type: none"> <li>Select a volume, and then click <b>Delete</b>.</li> <li>Click <b>Delete</b> again to confirm.</li> </ol>

## Resize a volume

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

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

## Modify the CIFS server

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

### Steps

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

Task	Action
DNS Primary and Secondary IP Address	<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> <p>If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.</p>
Active Directory Domain to join	<p>The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.</p>
Credentials authorized to join the domain	<p>The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.</p>
CIFS server NetBIOS name	<p>A CIFS server name that is unique in the AD domain.</p>
Organizational Unit	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <ul style="list-style-type: none"><li>• To configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter <b>OU=Computers,OU=corp</b> in this field.</li><li>• To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, enter <b>OU=AADDC Computers</b> or <b>OU=AADDC Users</b> in this field. <a href="#">Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</a></li><li>• To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter <b>OU=Computers,OU=Cloud</b> in this field. <a href="#">Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</a></li></ul>

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

3. Click **Save**.

## Result

Cloud Volumes ONTAP updates the CIFS server with the changes.

## Move a volume

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

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

## Steps

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

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

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

## Move a volume when Cloud Manager displays an Action Required message

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



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

## Steps

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

## Identify how to correct capacity issues

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

## Steps

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

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

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



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

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

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

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

4. If the system has reached the disk limit, do any of the following:
  - a. Delete any unused volumes.
  - b. Rearrange volumes to free space on an aggregate.

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

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

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

#### Move volumes to another system to avoid capacity issues

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

#### About this task

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



Moving a volume is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you because the system has reached the disk limit.

### Steps

1. Identify a Cloud Volumes ONTAP system that has available capacity, or deploy a new system.
2. Drag and drop the source working environment on the target working environment to perform a one-time data replication of the volume.

For details, see [Replicating data between systems](#).

3. Go to the Replication Status page, and then break the SnapMirror relationship to convert the replicated volume from a data protection volume to a read/write volume.

For details, see [Managing data replication schedules and relationships](#).

4. Configure the volume for data access.

For information about configuring a destination volume for data access, see the [ONTAP 9 Volume Disaster Recovery Express Guide](#).

5. Delete the original volume.

For details, see [Manage volumes](#).

### Move volumes to another aggregate to avoid capacity issues

You can move one or more volumes to another aggregate to avoid capacity issues.

### About this task

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

Moving two or more volumes is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you.

### Steps

1. Verify whether an existing aggregate has available capacity for the volumes that you need to move:
  - a. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
  - b. Select each aggregate, click **Info**, and then view the available capacity (aggregate capacity minus used aggregate capacity).

aggr1

Aggregate Capacity: 442.94 GB

Used Aggregate Capacity: 105.66 GB

2. If needed, add disks to an existing aggregate:
  - a. Select the aggregate, and then click **Add disks**.
  - b. Select the number of disks to add, and then click **Add**.
3. If no aggregates have available capacity, create a new aggregate.

For details, see [Creating aggregates](#).

4. Use System Manager or the CLI to move the volumes to the aggregate.
5. In most situations, you can use System Manager to move volumes.

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

### Reasons why a volume move might perform slowly

Moving a volume might take longer than you expect if any of the following conditions are true for Cloud Volumes ONTAP:

- The volume is a clone.
- The volume is a parent of a clone.
- The source or destination aggregate has a single Throughput Optimized HDD (st1) disk.
- One of the aggregates uses an older naming scheme for objects. Both aggregates have to use the same name format.

An older naming scheme is used if data tiering was enabled on an aggregate in the 9.4 release or earlier.

- The encryption settings don't match on the source and destination aggregates, or a rekey is in progress.
- The *-tiering-policy* option was specified on the volume move to change the tiering policy.
- The *-generate-destination-key* option was specified on the volume move.

### Tiering inactive data to low-cost object storage

You can reduce storage costs for Cloud Volumes ONTAP by combining an SSD or HDD performance tier for hot data with an object storage capacity tier for inactive data. Data tiering is powered by FabricPool technology. For a high-level overview, see [Data tiering overview](#).

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

1

**Choose a supported configuration**

Most configurations are supported. If you have a Cloud Volumes ONTAP system running the most recent version, then you should be good to go. [Learn more](#).

2

**Ensure connectivity between Cloud Volumes ONTAP and object storage**

- For AWS, you'll need a VPC Endpoint to S3. [Learn more](#).
- For Azure, you won't need to do anything as long as Cloud Manager has the required permissions. [Learn more](#).
- For Google Cloud, you need to configure the subnet for Private Google Access and set up a service account. [Learn more](#).

3

**Ensure that you have an aggregate with tiering enabled**

Data tiering must be enabled on an aggregate in order to enable data tiering on a volume. You should be aware of the requirements for new volumes and for existing volumes. [Learn more](#).

4

**Choose a tiering policy when creating, modifying, or replicating a volume**

Cloud Manager prompts you to choose a tiering policy when you create, modify, or replicate a volume.

- [Tiering data on read-write volumes](#)
- [Tiering data on data protection volumes](#)

**What's not required for data tiering?**

- You don't need to install a feature license to enable data tiering.
- You don't need to create an object store for the capacity tier. Cloud Manager does that for you.
- You don't need to enable data tiering at the system level.

Cloud Manager creates an object store for cold data when the system is created, [as long as there are no connectivity or permissions issues](#). After that, you just need to enable data tiering on volumes (and in some cases, [on aggregates](#)).

**Configurations that support data tiering**

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

**Support in AWS**

- Data tiering is supported in AWS starting with Cloud Volumes ONTAP 9.2.
- The performance tier can be General Purpose SSDs (gp3 or gp2) or Provisioned IOPS SSDs (io1).



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

## Support in Azure

- Data tiering is supported in Azure as follows:
  - Version 9.4 in with single node systems
  - Version 9.6 in with HA pairs
- The performance tier can be Premium SSD managed disks, Standard SSD managed disks, or Standard HDD managed disks.

## Support in Google Cloud

- Data tiering is supported in Google Cloud starting with Cloud Volumes ONTAP 9.6.
- The performance tier can be either SSD persistent disks, balanced persistent disks, or standard persistent disks.

## Feature interoperability

- Data tiering is supported with encryption technologies.
- Thin provisioning must be enabled on volumes.

## Requirements

Depending on your cloud provider, certain connections and permissions must be set up so that Cloud Volumes ONTAP can tier cold data to object storage.

### Requirements to tier cold data to AWS S3

Ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, see [AWS Documentation: Creating a Gateway Endpoint](#).

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

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

### Requirements to tier cold data to Azure Blob storage

You don't need to set up a connection between the performance tier and the capacity tier as long as Cloud Manager has the required permissions. Cloud Manager enables a VNet service endpoint for you if the Cloud Manager policy has these permissions:

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

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

### Requirements to tier cold data to a Google Cloud Storage bucket

- The subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access. For

instructions, refer to [Google Cloud Documentation: Configuring Private Google Access](#).

- You need a service account that meets the following requirements:
  - It must have the predefined Storage Admin role.
  - The Connector service account must be a *Service Account User* of this tiering service account.

[Learn how to set up a service account.](#)

- To encrypt the bucket with customer-managed encryption keys, enable the Google Cloud storage bucket to use the key.

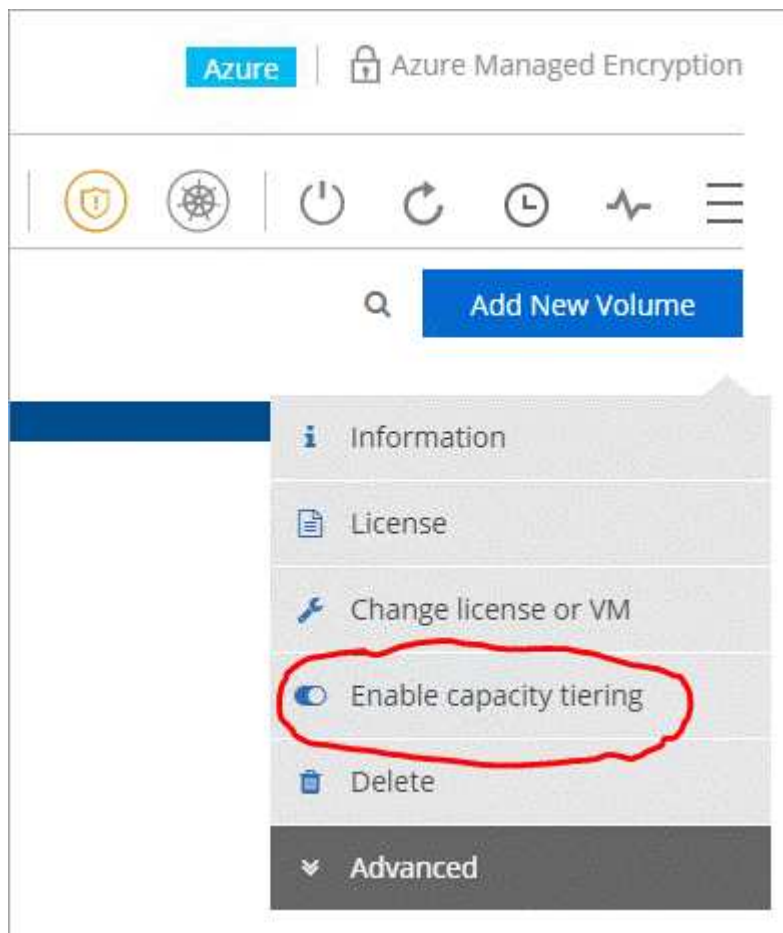
[Learn how to use customer-managed encryption keys with Cloud Volumes ONTAP.](#)

### Enabling data tiering after implementing the requirements

Cloud Manager creates an object store for cold data when the system is created, as long as there are no connectivity or permissions issues. If you didn't implement the requirements listed above until after you created the system, then you'll need to manually enable tiering, which creates the object store.

### Steps

1. [Ensure that you've met all requirements.](#)
2. On the Canvas page, double-click the name of the Cloud Volumes ONTAP instance.
3. Click the menu icon and select **Enable capacity tiering**.





You'll only see this option if data tiering couldn't be enabled when Cloud Manager created the system.

4. Click **Enable** so Cloud Manager can create the object store that this Cloud Volumes ONTAP system will use for tiered data.

## Ensuring that tiering is enabled on aggregates

Data tiering must be enabled on an aggregate in order to enable data tiering on a volume. You should be aware of the requirements for new volumes and for existing volumes.

### • New volumes

If you're enabling data tiering on a new volume, then you don't need to worry about enabling data tiering on an aggregate. Cloud Manager creates the volume on an existing aggregate that has tiering enabled, or it creates a new aggregate for the volume if a data tiering-enabled aggregate doesn't already exist.

### • Existing volumes

If you want to enable data tiering on an existing volume, then you'll need to ensure that data tiering is enabled on the underlying aggregate. If data tiering isn't enabled on the existing aggregate, then you'll need to use System Manager to attach an existing aggregate to the object store.

## Steps to confirm whether tiering is enabled on an aggregate

1. Open the working environment in Cloud Manager.
2. Click the menu icon, click **Advanced**, and then click **Advanced allocation**.
3. Verify whether tiering is enabled or disabled on the aggregate.

The screenshot shows the Cloud Manager interface for an aggregate named 'aggr1'. At the top, there are three server icons and the name 'aggr1', followed by a green 'ONLINE' status indicator. Below this, the interface is divided into two main sections: 'INFO' and 'CAPACITY'. The 'INFO' section contains a table with the following data:

INFO	
Disk Type	PREMIUM_LRS
Disks	1
Volumes	2
Tiering	Disabled

The 'Tiering' row is highlighted with a red rectangular box. The 'CAPACITY' section shows a progress bar for the disk, with a blue segment representing the used space. Below the progress bar, it indicates '1 TB' for 'Disk Allocated' and '143.36 GB' for 'Disk Used'.

## Steps to enable tiering on an aggregate

1. In System Manager, click **Storage > Tiers**.
2. Click the action menu for the aggregate and select **Attach Cloud Tiers**.
3. Select the cloud tier to attach and click **Save**.

## What's next?

You can now enable data tiering on new and existing volumes, as explained in the next section.

## Tiering data from read-write volumes

Cloud Volumes ONTAP can tier inactive data on read-write volumes to cost-effective object storage, freeing up the performance tier for hot data.

### Steps

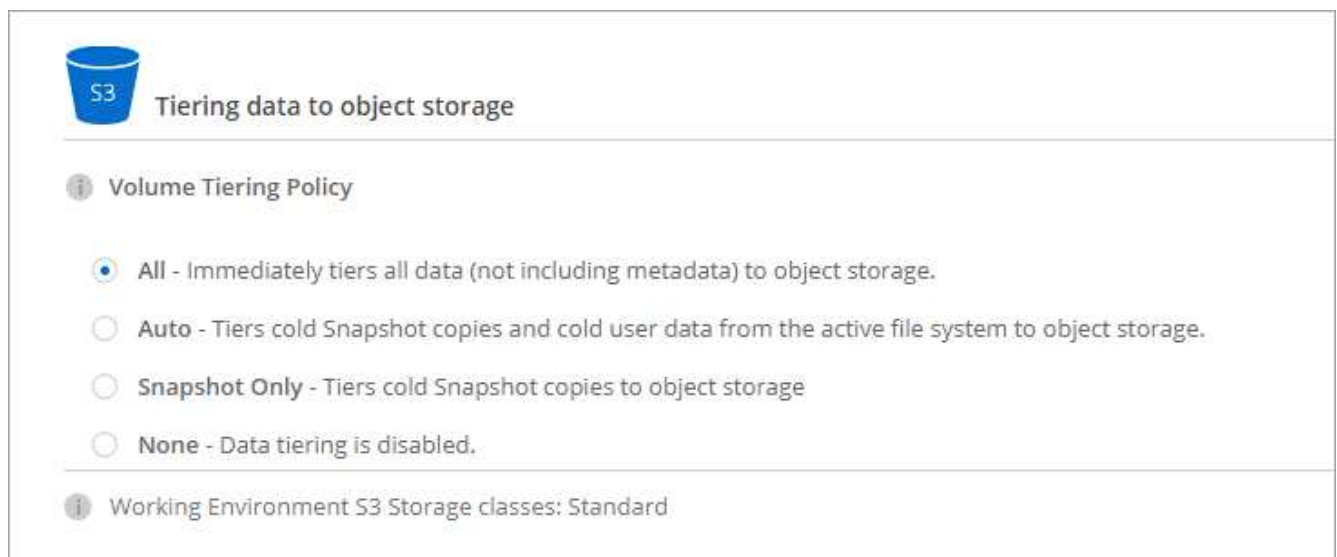
1. In the working environment, create a new volume or change the tier of an existing volume:

Task	Action
Create a new volume	Click <b>Add New Volume</b> .
Modify an existing volume	Select the volume and click <b>Change Disk Type &amp; Tiering Policy</b> .

2. Select a tiering policy.

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

### Example



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

## Tiering data from data protection volumes

Cloud Volumes ONTAP can tier data from a data protection volume to a capacity tier. If you activate the destination volume, the data gradually moves to the performance tier as it is read.

### Steps

1. On the Canvas page, select the working environment that contains the source volume, and then drag it to the working environment to which you want to replicate the volume.
2. Follow the prompts until you reach the tiering page and enable data tiering to object storage.

### Example


**S3 Tiering**
What are storage tiers?

☒ **Enabled**
☐ **Disabled**

**Note:** If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

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

## Changing the storage class for tiered data

After you deploy Cloud Volumes ONTAP, you can reduce your storage costs by changing the storage class for inactive data that hasn't been accessed for 30 days. The access costs are higher if you do access the data, so you must take that into consideration before you change the storage class.

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

For information about supported storage classes, see [Data tiering overview](#).

### Steps

1. From the working environment, click the menu icon and then click **Storage Classes** or **Blob Storage Tiering**.
2. Choose a storage class and then click **Save**.

## Changing the free space ratio for data tiering

The free space ratio for data tiering defines how much free space is required on Cloud Volumes ONTAP SSDs/HDDs when tiering data to object storage. The default setting is 10% free space, but you can tweak the setting based on your requirements.

For example, you might choose less than 10% free space to ensure that you are utilizing the purchased capacity. Cloud Manager can then purchase additional disks for you when additional capacity is required (up until you reach the disk limit for the aggregate).



If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data and you might experience performance degradation. Any change should be done with caution. If you're unsure, reach out to NetApp support for guidance.

The ratio is important for disaster recovery scenarios because as data is read from the object store, Cloud Volumes ONTAP moves the data to SSDs/HDDs to provide better performance. If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data. Take this into consideration when changing the ratio so that you can meet your business requirements.

### Steps

1. In the upper right of the Cloud Manager console, click the **Settings** icon, and select **Connector Settings**.





2. Under **Capacity**, click **Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering**.
3. Change the free space ratio based on your requirements and click **Save**.

### Changing the cooling period for the auto tiering policy

If you enabled data tiering on a Cloud Volumes ONTAP volume using the *auto* tiering policy, you can adjust the default cooling period based on your business needs. This action is supported using the API only.

The cooling period is the number of days that user data in a volume must remain inactive before it is considered "cold" and moved to object storage.

The default cooling period for the auto tiering policy is 31 days. You can change the cooling period as follows:

- 9.8 or later: 2 days to 183 days
- 9.7 or earlier: 2 days to 63 days

#### Step

1. Use the *minimumCoolingDays* parameter with your API request when creating a volume or modifying an existing volume.

### Connect a LUN to a host

When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

Note the following:

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

#### Steps

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

### Accelerate data access with FlexCache volumes

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

You can use FlexCache volumes to speed up access to data or to offload traffic from heavily accessed

volumes. FlexCache volumes help improve performance, especially when clients need to access the same data repeatedly, because the data can be served directly without having to access the origin volume. FlexCache volumes work well for system workloads that are read-intensive.

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

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

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



## Aggregate administration

### Create aggregates

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



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

### Steps

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

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

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

## Manage aggregates

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



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

### Before you begin


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

### About this task

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

### Steps

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

Task	Action
View information about an aggregate	Select an aggregate and click <b>Info</b> .
Create a volume on a specific aggregate	Select an aggregate and click <b>Create volume</b> .
Add disks to an aggregate	<ol style="list-style-type: none"> <li>a. Select an aggregate and click <b>Add disks</b>.</li> <li>b. Select the number of disks that you want to add and click <b>Add</b>.</li> </ol> <div>  All disks in an aggregate must be the same size. </div>
Delete an aggregate	<ol style="list-style-type: none"> <li>a. Select an aggregate that does not contain any volumes and click <b>Delete</b>.</li> <li>b. Click <b>Delete</b> again to confirm.</li> </ol>

# Storage VM administration

## Manage storage VMs in Cloud Manager

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but some configurations support additional storage VMs.

### Supported number of storage VMs

Multiple storage VMs are supported with certain configurations. Go to the [Cloud Volumes ONTAP Release Notes](#) to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

### Work with multiple storage VMs

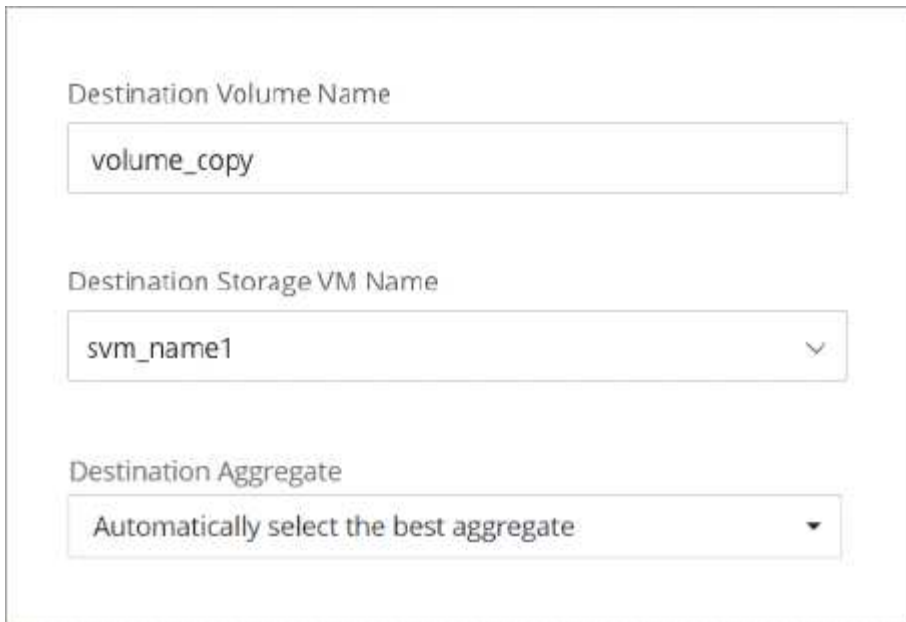
Cloud Manager supports any additional storage VMs that you create from System Manager or the CLI.

For example, the following image shows how you can choose a storage VM when you create a volume.



The screenshot shows a web form titled "Details & Protection". It contains three main sections: "Storage VM Name" with a dropdown menu showing "svm\_name1"; "Volume Name" and "Size (GiB)" with text input fields, the latter showing "Volume size"; and "Snapshot Policy" with a dropdown menu showing "default". There are information icons (i) next to the "Storage VM Name" and "Size (GiB)" labels. Below the "Snapshot Policy" dropdown, there is a link labeled "Default Policy" with an information icon.

And the following image shows how you can choose a storage VM when replicating a volume to another system.



Destination Volume Name

volume\_copy

Destination Storage VM Name

svm\_name1

Destination Aggregate

Automatically select the best aggregate

### Modify the name of the default storage VM

Cloud Manager automatically names the single storage VM that it creates for Cloud Volumes ONTAP. You can modify the name of the storage VM if you have strict naming standards. For example, you might want the name to match how you name the storage VMs for your ONTAP clusters.

If you created any additional storage VMs for Cloud Volumes ONTAP, then you can't rename the storage VMs from Cloud Manager. You'll need to do so directly from Cloud Volumes ONTAP by using System Manager or the CLI.

### Steps

1. From the working environment, click the menu icon, and then click **Information**.
2. Click the edit icon to the right of the storage VM name.



## Working Environment Information

### ONTAP

Serial Number:

[REDACTED]

System ID:

system-id-capacitytest

Cluster Name:

capacitytest

ONTAP Version:

9.7RC1

Date Created:

Jul 6, 2020 07:42:02 am

Storage VM Name:

svm\_capacitytest



3. In the Modify SVM Name dialog box, change the name, and then click **Save**.

### Manage storage VMs for disaster recovery

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

- [SVM Disaster Recovery Preparation Express Guide](#)
- [SVM Disaster Recovery Express Guide](#)

## Create data-serving storage VMs for Cloud Volumes ONTAP in AWS

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but some configurations support additional storage VMs.

To create additional data-serving storage VMs, you need to allocate IP addresses in AWS and then run ONTAP commands based on your Cloud Volumes ONTAP configuration.

### Supported number of storage VMs

Multiple storage VMs are supported with specific Cloud Volumes ONTAP configurations starting with the 9.7 release. Go to the [Cloud Volumes ONTAP Release Notes](#) to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All other Cloud Volumes ONTAP configurations support one data-serving storage VM and one destination storage VM used for disaster recovery. You can activate the destination storage VM for data access if there's

an outage on the source storage VM.

## Verify limits for your configuration

Each EC2 instance supports a maximum number of private IPv4 addresses per network interface. You need to verify the limit before you allocate IP addresses in AWS for the new storage VM.

### Steps

1. Go the [Storage limits section in the Cloud Volumes ONTAP Release Notes](#).
2. Identify the maximum number of IP addresses per interface for your instance type.
3. Make note of this number because you'll need it in the next section when you allocate IP addresses in AWS.

## Allocate IP addresses in AWS

Private IPv4 addresses must be assigned to port e0a in AWS before you create LIFs for the new storage VM.

Note that an optional management LIF for a storage VM requires a private IP address on a single node system and on an HA pair in a single AZ. This management LIF provides a connection to management tools like SnapCenter.

### Steps

1. Log in to AWS and open the EC2 service.
2. Select the Cloud Volumes ONTAP instance and click **Networking**.

If you're creating a storage VM on an HA pair, select node 1.

3. Scroll down to **Network interfaces** and click the **Interface ID** for port e0a.



4. Select the network interface and click **Actions > Manage IP addresses**.
5. Expand the list of IP addresses for e0a.
6. Verify the IP addresses:
  - a. Count the number of allocated IP addresses to confirm that the port has room for additional IPs.

You should have identified the maximum number of supported IP addresses per interface in the

previous section of this page.

- b. Optional: Go to the CLI for Cloud Volumes ONTAP and run **network interface show** to confirm that each of these IP addresses are in use.

If an IP address isn't in use, then you can use it with the new storage VM.

7. Back in the AWS Console, click **Assign new IP address** to assign additional IP addresses based on the amount that you need for the new storage VM.

- Single node system: One unused secondary private IP is required.

An optional secondary private IP is required if you want to create a management LIF on the storage VM.

- HA pair in a single AZ: One unused secondary private IP is required on node 1.

An optional secondary private IP is required if you want to create a management LIF on the storage VM.

- HA pair in multiple AZs: One unused secondary private IP is required on each node.

8. If you're allocating the IP address on an HA pair in a single AZ, enable **Allow secondary private IPv4 addresses to be reassigned**.

9. Click **Save**.

10. If you have an HA pair in multiple AZs, then you'll need to repeat these steps for node 2.

### Create a storage VM on a single node system

These steps create a new storage VM on a single node system. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

#### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. Create a NAS LIF.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node
```

Where *private\_ip\_x* is an unused secondary private IP on e0a.



### 3. Optional: Create a storage VM management LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

Where *private\_ip\_y* is another unused secondary private IP on e0a.

### 4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

## Create a storage VM on an HA pair in a single AZ

These steps create a new storage VM on an HA pair in a single AZ. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

Both of these LIFs get allocated on node 1. The private IP addresses can move between nodes if failures occur.

### Steps

#### 1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

#### 2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

Where *private\_ip\_x* is an unused secondary private IP on e0a of cvo-node1. This IP address can be relocated to the e0a of cvo-node2 in case of takeover because the service policy default-data-files indicates that IPs can migrate to the partner node.

#### 3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

Where *private\_ip\_y* is another unused secondary private IP on e0a.

#### 4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

### Create a storage VM on an HA pair in multiple AZs

These steps create a new storage VM on an HA pair in multiple AZs.

A *floating* IP address is required for a NAS LIF and is optional for a management LIF. These floating IP addresses don't require you to allocate private IPs in AWS. Instead, the floating IPs are automatically configured in the AWS route table to point to a specific node's ENI in the same VPC.

In order for floating IPs to work with ONTAP, a private IP address must be configured on every storage VM on each node. This is reflected in the steps below where an iSCSI LIF is created on node 1 and on node 2.

#### Steps

##### 1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

##### 2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

- The floating IP address must be outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. 192.168.209.27 is an example floating IP address. [Learn more about choosing a floating IP address.](#)
- `-service-policy default-data-files` indicates that IPs can migrate to the partner node.

### 3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

### 4. Create an iSCSI LIF on node 1.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask node1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

- This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
- `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.
- `private_ip` is an unused secondary private IP address on eth0 (e0a) of `cvo_node1`.

### 5. Create an iSCSI LIF on node 2.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

- This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
- `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.
- `private_ip` is an unused secondary private IP address on eth0 (e0a) of `cvo_node2`.

### 6. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

## Create data-serving storage VMs for Cloud Volumes ONTAP in Azure

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but additional storage VMs are supported when running Cloud Volumes ONTAP in Azure.

To create additional data-serving storage VMs, you need to allocate IP addresses in Azure and then run ONTAP commands to create the storage VM and data LIFs.

## Supported number of storage VMs

Multiple storage VMs are supported with specific Cloud Volumes ONTAP configurations starting with the 9.9.0 release. Go to the [Cloud Volumes ONTAP Release Notes](#) to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All other Cloud Volumes ONTAP configurations support one data-serving storage VM and one destination storage VM used for disaster recovery. You can activate the destination storage VM for data access if there's an outage on the source storage VM.

## Allocate IP addresses in Azure

You need to allocate IP addresses in Azure before you create a storage VM and allocate LIFs.

### Single node system

IP addresses must be assigned to nic0 in Azure before you create a storage VM and allocate LIFs. The number of IP addresses that you need depends on the storage protocol.

#### iSCSI

- One IP address for iSCSI data LIF access
- An optional IP address for a storage VM (SVM) management LIF

This management LIF provides a connection to management tools like SnapCenter.

#### NFS

- One IP address for NAS data LIF access
- An optional IP address for a storage VM (SVM) management LIF

This management LIF provides a connection to management tools like SnapCenter.

#### SMB

- One IP address for NAS data LIF access
- One IP address for DNS and SMB communication through an iSCSI LIF

An iSCSI LIF is used for this purpose because it doesn't migrate on failover.

- An optional IP address for a storage VM (SVM) management LIF

This management LIF provides a connection to management tools like SnapCenter.

## Steps

1. Log in to the Azure portal and open the **Virtual machine** service.
2. Click the name of the Cloud Volumes ONTAP VM.
3. Click **Networking**.

4. Click the name of the network interface for nic0.
5. Under **Settings**, click **IP configurations**.
6. Click **Add**.
7. Enter a name for the IP configuration, select **Dynamic**, and then click **OK**.
8. Click the name of the IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

9. If you're using SMB, repeat these steps to create an additional IP address for DNS and SMB communication.
10. If you want to create an SVM management LIF, repeat these steps to create an additional IP address.

### **After you finish**

Copy the private IP addresses that you just created. You'll need to specify those IP addresses when you create LIFs for the new storage VM.

### **HA pair**

How you allocate IP addresses for an HA pair depends on the storage protocol that you're using.

## iSCSI

iSCSI IP addresses must be assigned to nic0 in Azure before you create a storage VM and allocate LIFs. IPs for iSCSI are assigned to nic0 and not the load balancer because iSCSI uses ALUA for failover.

You'll need to create the following IP addresses:

- One IP address for iSCSI data LIF access from node 1
- One IP address for iSCSI data LIF access from node 2
- An optional IP address for a storage VM (SVM) management LIF

This management LIF provides a connection to management tools like SnapCenter.

### Steps

1. Log in to the Azure portal and open the **Virtual machine** service.
2. Click the name of the Cloud Volumes ONTAP VM for node 1.
3. Click **Networking**.
4. Click the name of the network interface for nic0.
5. Under **Settings**, click **IP configurations**.
6. Click **Add**.
7. Enter a name for the IP configuration, select **Dynamic**, and then click **OK**.
8. Click the name of the IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

9. Repeat these steps on node 2.
10. If you want to create an SVM management LIF, repeat these steps on node 1.

## NFS

IP addresses that you use for NFS are allocated in the load balancer so that the IP addresses can migrate to the other node in case failover events occur.

You'll need to create the following IP addresses:

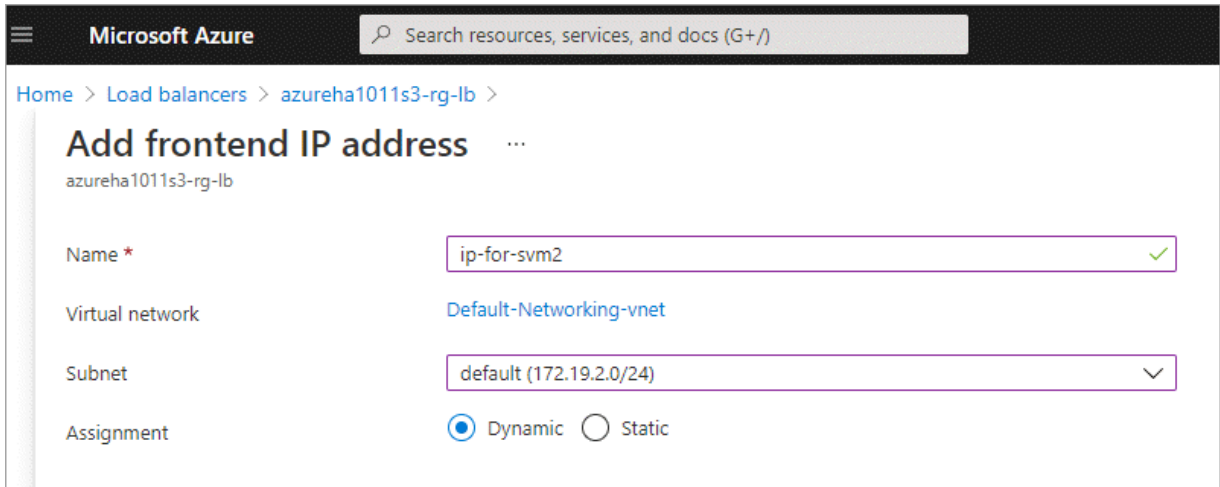
- One IP address for NAS data LIF access from node 1
- One IP address for NAS data LIF access from node 2
- An optional IP address for a storage VM (SVM) management LIF

This management LIF provides a connection to management tools like SnapCenter.

### Steps

1. In the Azure portal, open the **Load balancers** service.
2. Click the name of the load balancer for the HA pair.
3. Create one frontend IP configuration for data LIF access from node 1, another for data LIF access from node 2, and another optional frontend IP for a storage VM (SVM) management LIF.

- a. Under **Settings**, click **Frontend IP configuration**.
- b. Click **Add**.
- c. Enter a name for the frontend IP, select the subnet for the Cloud Volumes ONTAP HA pair, and leave **Dynamic** selected.



The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and the Microsoft Azure logo. Below the navigation bar, the breadcrumb trail reads: Home > Load balancers > azureha1011s3-rg-lb >. The main heading is 'Add frontend IP address' with a three-dot menu icon to its right. Below the heading, the resource name 'azureha1011s3-rg-lb' is displayed. The configuration form includes the following fields:

- Name \***: A text input field containing 'ip-for-svm2' with a green checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet**: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and 'Static'.

- d. Click the name of the frontend IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

4. Add a health probe for each frontend IP that you just created.
  - a. Under the load balancer's **Settings**, click **Health probes**.
  - b. Click **Add**.
  - c. Enter a name for the health probe and enter a port number that's between 63005 and 65000. Keep the default values for the other fields.

It's important that the port number is between 63005 and 65000. For example, if you are creating three health probes, you could enter probes that use the port numbers 63005, 63006, and 63007.

Microsoft Azure

Search resources, services, and

[Home](#) > [Load balancers](#) > [azureha1011s3-rg-lb](#) >

## Add health probe

azureha1011s3-rg-lb

Name *	svm2-health-probe1	✓
Protocol *	TCP	▼
Port * ⓘ	63005	✓
Interval * ⓘ	5	seconds
Unhealthy threshold * ⓘ	2	consecutive failures
Used by ⓘ	Not used	

5. Create new load balancing rules for each frontend IP.
  - a. Under the load balancer's **Settings**, click **Load balancing rules**.
  - b. Click **Add** and enter the required information:
    - **Name**: Enter a name for the rule.
    - **IP Version**: Select **IPv4**.
    - **Frontend IP address**: Select one of the frontend IP addresses that you just created.
    - **HA Ports**: Enable this option.
    - **Backend pool**: Keep the default Backend pool that was already selected.
    - **Health probe**: Select the health probe that you created for the selected frontend IP.
    - **Session persistence**: Select **None**.
    - **Floating IP**: Select **Enabled**.



## Add load balancing rule

chandanaTcpRst3-rg-lb

**i** A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name \*

jimmy\_new\_rule ✓

IP Version \*

☒ IPv4 ☐ IPv6

Frontend IP address \* ⓘ

10.1.0.156 (dataAFIP) ▼

☒ HA Ports ⓘ

Backend pool ⓘ

backendPool (2 virtual machines) ▼

Health probe ⓘ

dataProbe (TCP:63002) ▼

Session persistence ⓘ

None ▼

Floating IP ⓘ

☐ Disabled ☒ Enabled

6. Ensure that the network security group rules for Cloud Volumes ONTAP allows the load balancer to send TCP probes for the health probes that were created in step 4 above. Note that this is allowed by default.

### SMB

IP addresses that you use for SMB data are allocated in the load balancer so that the IP addresses can migrate to the other node in case failover events occur.

You'll need to create the following IP addresses:

- One IP address for NAS data LIF access from node 1
- One IP address for NAS data LIF access from node 2
- One IP address for an iSCSI LIF on node 1
- One IP address for an iSCSI LIF on node 2

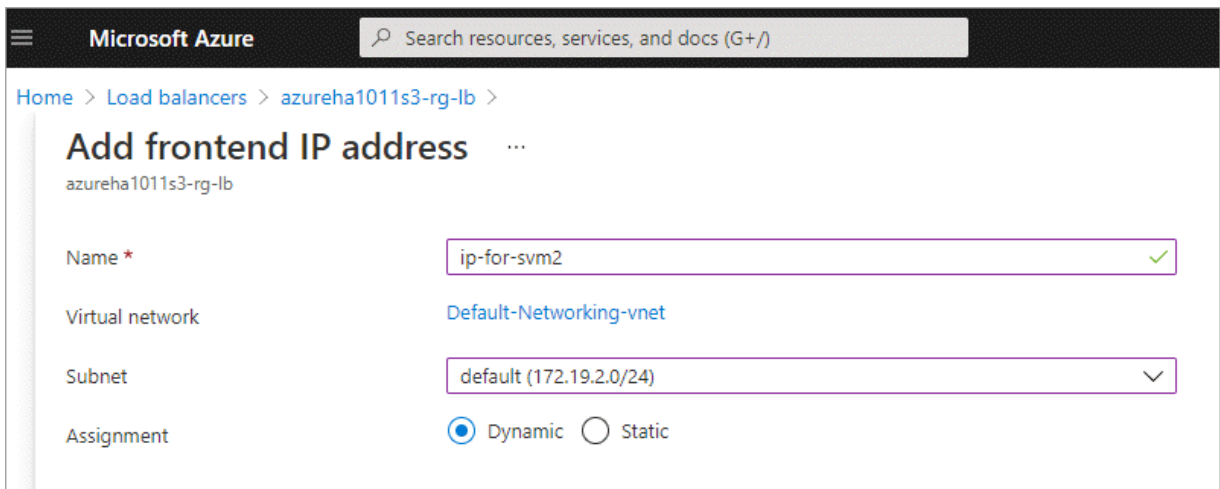
The iSCSI LIFs are required for DNS and SMB communication. An iSCSI LIF is used for this purpose because it doesn't migrate on failover.

- An optional IP address for a storage VM (SVM) management LIF

This management LIF provides a connection to management tools like SnapCenter.

## Steps

1. In the Azure portal, open the **Load balancers** service.
2. Click the name of the load balancer for the HA pair.
3. Create the required number of frontend IP configurations:
  - a. Under **Settings**, click **Frontend IP configuration**.
  - b. Click **Add**.
  - c. Enter a name for the frontend IP, select the subnet for the Cloud Volumes ONTAP HA pair, and leave **Dynamic** selected.



The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and the Microsoft Azure logo. Below the navigation bar, the breadcrumb trail reads: Home > Load balancers > azureha1011s3-rg-lb >. The main heading is 'Add frontend IP address' with a three-dot menu icon. Below the heading, the resource name 'azureha1011s3-rg-lb' is displayed. The configuration form includes the following fields:

- Name \***: A text input field containing 'ip-for-svm2' with a green checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet**: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and 'Static'.

- d. Click the name of the frontend IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

4. Add a health probe for each frontend IP that you just created.
  - a. Under the load balancer's **Settings**, click **Health probes**.
  - b. Click **Add**.
  - c. Enter a name for the health probe and enter a port number that's between 63005 and 65000. Keep the default values for the other fields.

It's important that the port number is between 63005 and 65000. For example, if you are creating three health probes, you could enter probes that use the port numbers 63005, 63006, and 63007.

Microsoft Azure

Search resources, services, and

[Home](#) > [Load balancers](#) > [azureha1011s3-rg-lb](#) >

## Add health probe

azureha1011s3-rg-lb

Name *	svm2-health-probe1	✓
Protocol *	TCP	▼
Port * ⓘ	63005	✓
Interval * ⓘ	5	seconds
Unhealthy threshold * ⓘ	2	consecutive failures
Used by ⓘ	Not used	

5. Create new load balancing rules for each frontend IP.
  - a. Under the load balancer's **Settings**, click **Load balancing rules**.
  - b. Click **Add** and enter the required information:
    - **Name**: Enter a name for the rule.
    - **IP Version**: Select **IPv4**.
    - **Frontend IP address**: Select one of the frontend IP addresses that you just created.
    - **HA Ports**: Enable this option.
    - **Backend pool**: Keep the default Backend pool that was already selected.
    - **Health probe**: Select the health probe that you created for the selected frontend IP.
    - **Session persistence**: Select **None**.
    - **Floating IP**: Select **Enabled**.

## Add load balancing rule

chandanaTcpRst3-rg-lb

**i** A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name \*

jimmy\_new\_rule

IP Version \*



IPv4



IPv6

Frontend IP address \* ⓘ

10.1.0.156 (dataAFIP)

☒ HA Ports ⓘ

Backend pool ⓘ

backendPool (2 virtual machines)

Health probe ⓘ

dataAProbe (TCP:63002)

Session persistence ⓘ

None

Floating IP ⓘ

Disabled

Enabled

6. Ensure that the network security group rules for Cloud Volumes ONTAP allows the load balancer to send TCP probes for the health probes that were created in step 4 above. Note that this is allowed by default.

### After you finish

Copy the private IP addresses that you just created. You'll need to specify those IP addresses when you create LIFs for the new storage VM.

### Create a storage VM and LIFs

After you allocate IP addresses in Azure, you can create a new storage VM on a single node system or on an HA pair.

#### Single node system

How you create a storage VM and LIFs on a single node system depends on the storage protocol that you're using.

## iSCSI

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Create a data LIF:

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data  
-protocol iscsi
```

3. Optional: Create a storage VM management LIF.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node node1 -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert  
false -failover-group Default
```

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

## NFS

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

## 2. Create a data LIF:

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy disabled -firewall-policy data -home-port e0a -auto  
-revert true -failover-group Default
```

## 3. Optional: Create a storage VM management LIF.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node node1 -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert  
false -failover-group Default
```

## 4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

## SMB

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

#### 1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. Create a data LIF:

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. Create an iSCSI LIF that is required to provide DNS and SMB communication:

```
network interface create -vserver <svm-name> -home-port e0a -address
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data
-protocol iscsi
```

4. Optional: Create a storage VM management LIF.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node node1 -status-admin up -failover-policy
system-defined -firewall-policy mgmt -home-port e0a -auto-revert
false -failover-group Default
```

5. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

## HA pair

How you create a storage VM and LIFs on an HA pair depends on the storage protocol that you're using.

## iSCSI

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Create data LIFs:

- a. Use the following command to create an iSCSI LIF on node 1.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node1> -data-protocol iscsi
```

- b. Use the following command to create an iSCSI LIF on node 2.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node2> -data-protocol iscsi
```

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node node1 -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert  
false -failover-group Default
```

This management LIF provides a connection to management tools like SnapCenter.

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you



can create volumes on the storage VM.

## NFS

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Create data LIFs:

- a. Use the following command to create a NAS LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-ip-address>  
-netmask-length <length> -home-node <name-of-node1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

- b. Use the following command to create a NAS LIF on node 2.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node node1 -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert  
false -failover-group Default -probe-port <port-number-for-azure-  
health-probe3>
```

This management LIF provides a connection to management tools like SnapCenter.

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

## SMB

Follow these steps to create a new storage VM, along with the required LIFs.

### Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. Create NAS data LIFs:

- a. Use the following command to create a NAS LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs--ip-address>  
-netmask-length <length> -home-node <name-of-node1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

- b. Use the following command to create a NAS LIF on node 2.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

3. Create iSCSI LIFs to provide DNS and SMB communication:

- a. Use the following command to create an iSCSI LIF on node 1.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node1> -data-protocol iscsi
```

- b. Use the following command to create an iSCSI LIF on node 2.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node2> -data-protocol iscsi
```

4. Optional: Create a storage VM management LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node node1 -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert  
false -failover-group Default -probe-port <port-number-for-azure-  
health-probe3>
```

This management LIF provides a connection to management tools like SnapCenter.

5. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

### What's next?

After you create a storage VM on an HA pair, it's best to wait 12 hours before you provision storage on that SVM. Starting with the Cloud Volumes ONTAP 9.10.1 release, Cloud Manager scans the settings for an HA pair's load balancer at a 12-hour interval. If there are new SVMs, Cloud Manager will enable a setting that provides shorter unplanned failover.

## Security and data encryption

### Encrypting volumes with NetApp encryption solutions

Cloud Volumes ONTAP supports NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE). NVE and NAE are software-based solutions that enable FIPS 140-2–compliant data-at-rest encryption of volumes. [Learn more about these](#)

## encryption solutions.

Both NVE and NAE are supported with an external key manager.

If you use NVE, you have the option to use your cloud provider's key vault to protect ONTAP encryption keys:

- [Azure Key Vault \(AKV\)](#)
- [Google Cloud Key Management Service](#)

New aggregates will have NAE enabled by default after you set up an external key manager. New volumes that aren't part of an NAE aggregate will have NVE enabled by default (for example, if you have existing aggregates that were created before setting up an external key manager).

Cloud Volumes ONTAP doesn't support onboard key management.

### What you'll need

Your Cloud Volumes ONTAP system should be registered with NetApp support. A NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support.

- [Adding NetApp Support Site accounts to Cloud Manager](#)
- [Registering pay-as-you-go systems](#)



Cloud Manager doesn't install the NVE license on systems that reside in the China region.

### Steps

1. Review the list of supported key managers in the [NetApp Interoperability Matrix Tool](#).



Search for the **Key Managers** solution.

2. [Connect to the Cloud Volumes ONTAP CLI](#).
3. Configure external key management.
  - [Azure Key Vault \(AKV\)](#)
  - [Google Cloud Key Management Service](#)

## Manage keys with Azure Key Vault

You can use [Azure Key Vault \(AKV\)](#) to protect your ONTAP encryption keys in an Azure-deployed application.

AKV can be used to protect [NetApp Volume Encryption \(NVE\) keys](#) only for data SVMs.

Key management with AKV can be enabled with the CLI or the ONTAP REST API.

When using AKV, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (login.microsoftonline.com). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

### Prerequisites

- Cloud Volumes ONTAP must be running version 9.10.1 or later

- Volume Encryption (VE) license installed (NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support.)
- Multi-tenant Encryption Key Management (MTEKM) license installed
- You must be a cluster or SVM administrator
- An Active Azure subscription

## Limitations

- AKV can only be configured on a data SVM

## Configuration process

The outlined steps capture how to register your Cloud Volumes ONTAP configuration with Azure and how to create an Azure Key Vault and keys. If you have already completed these steps, ensure you have the correct configuration settings, particularly in [Create an Azure Key Vault](#), and then proceed to [Cloud Volumes ONTAP configuration](#).

- \* [Azure Application Registration](#)
- \* [Create Azure client secret](#)
- \* [Create an Azure Key Vault](#)
- \* [Create encryption key](#)
- \* [Create an Azure Active Directory Endpoint \(HA only\)](#)
- \* [Cloud Volumes ONTAP configuration](#)

## Azure Application Registration

1. You must first register your application in the Azure subscription that you want the Cloud Volumes ONTAP to use for access the Azure Key Vault. Within the Azure portal, select **App registrations**.
2. Select **New registration**.
3. Provide a name for your application and select a supported application type. The default single tenant suffices for Azure Key Vault usage. Select **Register**.
4. In the Azure Overview window, select the application you have registered. Copy the **application (client) ID** and the **directory (tenant) ID** to a secure location. They will be required later in the registration process.

## Create Azure client secret

1. In the Azure portal for your Cloud Volumes ONTAP application, select the **Certificates & secrets** pane.
2. Select **New client secret** Enter a meaningful name for your client secret. NetApp recommends a 24-month expiration period, however your specific cloud governance policies may require a different setting.
3. Select **Add** to save the client secret. Immediately copy the **Value** of the secret and store it somewhere secure for future configuration. The secret value will not be displayed after you navigate away from the page.

## Create an Azure Key Vault

1. If you have an existing Azure Key Vault, you can connect it to your Cloud Volumes ONTAP configuration, however you must adapt the access policies to the settings in this process.
2. In the Azure portal, navigate to the **Key Vaults** section.
3. Select **Create**. Enter the required information including resource group, region and pricing tier and make selections for the days to retain deleted vaults and whether or not purge protection is enabled. For the purposes of this configuration, defaults are sufficient, however your specific cloud governance policies may require different settings.
4. Select **Next** to choose an access policy.

5. Select **Azure Disk Encryption** for the volume encryption option and **Vault access policy** for the permission model.
6. Select **Add Access Policy**.
7. Select the caret adjacent to the **Configure from template (optional)** field. Then, select **Key, Secret, & Certification Management**.
8. Choose each of the drop-down permissions menus (key, secret, certificate) and then **Select all** at the top of the menu list to select all the permissions available. You should have:
  - **Key permissions:** 19 selected
  - **Secret permissions:** 8 selected
  - **Certificate permissions:** 16 selected
9. Select **Add** to create the access policy.
10. Select **Next** to advance to **Networking** options.
11. Choose the appropriate network access method or select **All networks** and **Review + Create** to create the key vault. (Network access method may be prescribed by a governance policy or your corporate cloud security team.)
12. Record the Key Vault URI: In the key vault you created, navigate to the Overview menu and copy the **Vault URI** from the right-hand column. You will need this for a later step.

#### Create encryption key

1. In the menu for the Key Vault you have created for Cloud Volumes ONTAP, navigate to the **Keys** option.
2. Select **Generate/import** to create a new key.
3. Leave the default option set to **Generate**.
4. Provide the following information:
  - Encryption key name
  - Key type: RSA
  - RSA key size: 2048
  - Enabled: Yes
5. Select **Create** to create the encryption key.
6. Return to the **Keys** menu and select the key you just created.
7. Select the key ID under **Current version** to view the key properties.
8. Locate the **Key Identifier** field. Copy the URI up to but not including the hexadecimal string.

#### Create an Azure Active Directory Endpoint (HA only)

1. This process is only required if you are configuring Azure Key Vault for an HA Cloud Volumes ONTAP Working Environment.
2. In the Azure portal navigate to **Virtual Networks**.
3. Select the Virtual Network where you deployed the Cloud Volumes ONTAP working environment and select the **Subnets** menu on the left side of the page.
4. Select the subnet name for your Cloud Volumes ONTAP deployment from the list.
5. Navigate to the **Service Endpoints** heading. In the dropdown menu, select **Microsoft.AzureActiveDirectory** from the list.
6. Select **Save** to capture your settings.

## Cloud Volumes ONTAP configuration

1. Connect to the cluster management LIF with your preferred SSH client.
2. Enter the advanced privilege mode in ONTAP:  
`set advanced -con off``
3. Identify the desired data SVM and verify its DNS configuration:  
`vserver services name-service dns show`
  - a. If a DNS entry for the desired data SVM exists and it contains an entry for the Azure DNS, then no action is required. If it does not, add a DNS server entry for the data SVM that points to the Azure DNS, private DNS, or on-premise server. This should match the entry for the cluster admin SVM:  
`vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`
  - b. Verify the DNS service has been created for the data SVM:  
`vserver services name-service dns show`
4. Enable Azure Key Vault using the client ID and tenant ID saved after the application registration:  
`security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name Azure_key_name -key-id Azure_key_ID`
5. Verify the key manager configuration:  
`security key-manager external azure show`
6. Check the status of the key manager:  
`security key-manager external azure check`  
The output will look like:

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
Status: OK

Category: ekmip_server
Status: OK

Category: kms_wrapped_key_status
Status: UNKNOWN
Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

If the `service_reachability` status is not OK, the SVM cannot reach the Azure Key Vault service with all the required connectivity and permissions.

The `kms_wrapped_key_status` will report UNKNOWN at initial configuration. Its status will change to OK after the first volume is encrypted.

7. OPTIONAL: Create a test volume to verify the functionality of AKV.

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size  
-state online -policy default
```

If configured correctly, Cloud Volumes ONTAP will automatically create the volume and enable volume encryption.

1. Confirm the volume was created and encrypted correctly. If it is, the `-is-encrypted` parameter will display as `true`.

```
vol show -vserver SVM_name -fields is-encrypted
```

## Manage keys with Google's Cloud Key Management Service

You can use [Google Cloud Platform's Key Management Service \(Cloud KMS\)](#) to protect your ONTAP encryption keys in a Google Cloud Platform-deployed application.

Key management with Cloud KMS can be enabled with the CLI or the ONTAP REST API.

When using Cloud KMS, be aware that by default a data SVMs LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services ([oauth2.googleapis.com](#)). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

### Prerequisites

- Cloud Volumes ONTAP must be running version 9.10.1 or later
- Volume Encryption (VE) license installed
- Multi-tenant Encryption Key Management (MTEKM) license installed
- You must be a cluster or SVM administrator
- An active Google Cloud Platform subscription

### Limitations

- Cloud KMS can only be configured on a data SVM

### Configuration

#### Google Cloud

1. In your Google Cloud environment, [create a symmetric GCP key ring and key](#).
2. Create a custom role for your Cloud Volumes ONTAP service account.



```
gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

  --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
  list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
  useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
  tions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

3. Assign the custom role to the Cloud KMS key and Cloud Volumes ONTAP service account:

```
gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
--location key_location --member serviceAccount:_service_account_Name_ --role
projects/customer_project_id/roles/kmsCustomRole
```

4. Download service account JSON key:

```
gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com
```

## Cloud Volumes ONTAP

1. Connect to the cluster management LIF with your preferred SSH client.

2. Switch to the advanced privilege level:

```
set -privilege advanced
```

3. Create a DNS for the data SVM.

```
dns create -domains c.<project>.internal -name-servers server_address -vserver
SVM_name
```

4. Create CMEK entry:

```
security key-manager external gcp enable -vserver SVM_name -project-id project
-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name
key_name
```

5. When prompted, enter the service account JSON key from your GCP account.

6. Confirm the enabled process succeeded:

```
security key-manager external gcp check -vserver svm_name
```

7. OPTIONAL: Create a volume to test encryption `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

## Troubleshoot

If you need to troubleshoot, you can tail the raw REST API logs in the final two steps above:

```
.set d
.systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log
```

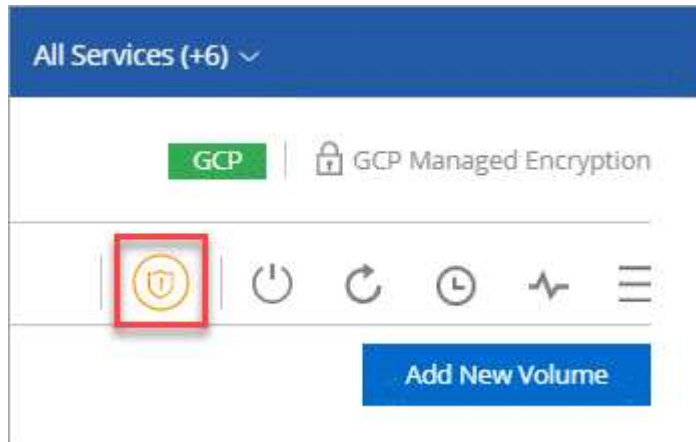
## Improving protection against ransomware

Ransomware attacks can cost a business time, resources, and reputation. Cloud

Manager enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

### Steps

1. From the working environment, click the **Ransomware** icon.



2. Implement the NetApp solution for ransomware:

- a. Click **Activate Snapshot Policy**, if you have volumes that do not have a Snapshot policy enabled.

NetApp Snapshot technology provides the industry's best solution for ransomware remediation. The key to a successful recovery is restoring from uninfected backups. Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

- b. Click **Activate FPolicy** to enable ONTAP's FPolicy solution, which can block file operations based on a file's extension.

This preventative solution improves protection from ransomware attacks by blocking common ransomware file types.

The default FPolicy scope blocks files that have the following extensions:

micro, encrypted, locked, crypto, crypt, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, good, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre



Cloud Manager creates this scope when you activate FPolicy on Cloud Volumes ONTAP. The list is based on common ransomware file types. You can customize the blocked file extensions by using the `vserver fpolicy policy scope` commands from the Cloud Volumes ONTAP CLI.

### Ransomware Protection

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

#### 1 Enable Snapshot Copy Protection

50 %  
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes.

Activate Snapshot Policy

#### 2 Block Ransomware File Extensions



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

[View Denied File Names](#)

Activate FPolicy

## Manage keys with Azure Key Vault

You can use [Azure Key Vault \(AKV\)](#) to protect your ONTAP encryption keys in an Azure-deployed application.

AKV can be used to protect [NetApp Volume Encryption \(NVE\) keys](#) only for data SVMs.

Key management with AKV can be enabled with the CLI or the ONTAP REST API.

When using AKV, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (login.microsoftonline.com). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

### Prerequisites

- Cloud Volumes ONTAP must be running version 9.10.1 or later
- Volume Encryption (VE) license installed (NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support.)
- Multi-tenant Encryption Key Management (MTEKM) license installed
- You must be a cluster or SVM administrator
- An Active Azure subscription

### Limitations

- AKV can only be configured on a data SVM

### Configuration process

The outlined steps capture how to register your Cloud Volumes ONTAP configuration with Azure and how to create an Azure Key Vault and keys. If you have already completed these steps, ensure you have the correct configuration settings, particularly in [Create an Azure Key Vault](#), and then proceed to [Cloud Volumes ONTAP configuration](#).

- \* [Azure Application Registration](#)
- \* [Create Azure client secret](#)
- \* [Create an Azure Key Vault](#)
- \* [Create encryption key](#)
- \* [Create an Azure Active Directory Endpoint \(HA only\)](#)

## Azure Application Registration

1. You must first register your application in the Azure subscription that you want the Cloud Volumes ONTAP to use for access the Azure Key Vault. Within the Azure portal, select **App registrations**.
2. Select **New registration**.
3. Provide a name for your application and select a supported application type. The default single tenant suffices for Azure Key Vault usage. Select **Register**.
4. In the Azure Overview window, select the application you have registered. Copy the **application (client) ID** and the **directory (tenant) ID** to a secure location. They will be required later in the registration process.

## Create Azure client secret

1. In the Azure portal for your Cloud Volumes ONTAP application, select the **Certificates & secrets** pane.
2. Select **New client secret** Enter a meaningful name for your client secret. NetApp recommends a 24-month expiration period, however your specific cloud governance policies may require a different setting.
3. Select **Add** to save the client secret. Immediately copy the **Value** of the secret and store it somewhere secure for future configuration. The secret value will not be displayed after you navigate away from the page.

## Create an Azure Key Vault

1. If you have an existing Azure Key Vault, you can connect it to your Cloud Volumes ONTAP configuration, however you must adapt the access policies to the settings in this process.
2. In the Azure portal, navigate to the **Key Vaults** section.
3. Select **Create**. Enter the required information including resource group, region and pricing tier and make selections for the days to retain deleted vaults and whether or not purge protection is enabled. For the purposes of this configuration, defaults are sufficient, however your specific cloud governance policies may require different settings.
4. Select **Next** to choose an access policy.
5. Select **Azure Disk Encryption** for the volume encryption option and **Vault access policy** for the permission model.
6. Select **Add Access Policy**.
7. Select the caret adjacent to the **Configure from template (optional)** field. Then, select **Key, Secret, & Certification Management**.
8. Choose each of the drop-down permissions menus (key, secret, certificate) and then **Select all** at the top of the menu list to select all the permissions available. You should have:
  - **Key permissions:** 19 selected
  - **Secret permissions:** 8 selected
  - **Certificate permissions:** 16 selected
9. Select **Add** to create the access policy.
10. Select **Next** to advance to **Networking** options.
11. Choose the appropriate network access method or select **All networks** and **Review + Create** to create the key vault. (Network access method may be prescribed by a governance policy or your corporate cloud security team.)
12. Record the Key Vault URI: In the key vault you created, navigate to the Overview menu and copy the **Vault URI** from the right-hand column. You will need this for a later step.

## Create encryption key

1. In the menu for the Key Vault you have created for Cloud Volumes ONTAP, navigate to the **Keys** option.
2. Select **Generate/import** to create a new key.
3. Leave the default option set to **Generate**.
4. Provide the following information:
  - Encryption key name
  - Key type: RSA
  - RSA key size: 2048
  - Enabled: Yes
5. Select **Create** to create the encryption key.
6. Return to the **Keys** menu and select the key you just created.
7. Select the key ID under **Current version** to view the key properties.
8. Locate the **Key Identifier** field. Copy the URI up to but not including the hexadecimal string.

## Create an Azure Active Directory Endpoint (HA only)

1. This process is only required if you are configuring Azure Key Vault for an HA Cloud Volumes ONTAP Working Environment.
2. In the Azure portal navigate to **Virtual Networks**.
3. Select the Virtual Network where you deployed the Cloud Volumes ONTAP working environment and select the **Subnets** menu on the left side of the page.
4. Select the subnet name for your Cloud Volumes ONTAP deployment from the list.
5. Navigate to the **Service Endpoints** heading. In the dropdown menu, select **Microsoft.AzureActiveDirectory** from the list.
6. Select **Save** to capture your settings.

## Cloud Volumes ONTAP configuration

1. Connect to the cluster management LIF with your preferred SSH client.
2. Enter the advanced privilege mode in ONTAP:  
`set advanced -con off``
3. Identify the desired data SVM and verify its DNS configuration:  
`vserver services name-service dns show`
  - a. If a DNS entry for the desired data SVM exists and it contains an entry for the Azure DNS, then no action is required. If it does not, add a DNS server entry for the data SVM that points to the Azure DNS, private DNS, or on-premise server. This should match the entry for the cluster admin SVM:  
`vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`
  - b. Verify the DNS service has been created for the data SVM:  
`vserver services name-service dns show`
4. Enable Azure Key Vault using the client ID and tenant ID saved after the application registration:  
`security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name Azure_key_name -key-id Azure_key_ID`

5. Verify the key manager configuration:

```
security key-manager external azure show
```

6. Check the status of the key manager:

```
security key-manager external azure check
```

The output will look like:

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
Status: OK

Category: ekvip_server
Status: OK

Category: kms_wrapped_key_status
Status: UNKNOWN
Details: No volumes created yet for the vsriver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

If the `service_reachability` status is not OK, the SVM cannot reach the Azure Key Vault service with all the required connectivity and permissions.

The `kms_wrapped_key_status` will report UNKNOWN at initial configuration. Its status will change to OK after the first volume is encrypted.

7. OPTIONAL: Create a test volume to verify the functionality of AKV.

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
-state online -policy default
```

If configured correctly, Cloud Volumes ONTAP will automatically create the volume and enable volume encryption.

1. Confirm the volume was created and encrypted correctly. If it is, the `-is-encrypted` parameter will display as `true`.

```
vol show -vserver SVM_name -fields is-encrypted
```

## Manage keys with Google's Cloud Key Management Service

You can use [Google Cloud Platform's Key Management Service \(Cloud KMS\)](#) to protect your ONTAP encryption keys in a Google Cloud Platform-deployed application.

Key management with Cloud KMS can be enabled with the CLI or the ONTAP REST API.

When using Cloud KMS, be aware that by default a data SVMs LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's

authentication services (oauth2.googleapis.com). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

### Prerequisites

- Cloud Volumes ONTAP must be running version 9.10.1 or later
- Volume Encryption (VE) license installed
- Multi-tenant Encryption Key Management (MTEKM) license installed
- You must be a cluster or SVM administrator
- An active Google Cloud Platform subscription

### Limitations

- Cloud KMS can only be configured on a data SVM

### Configuration

#### Google Cloud

1. In your Google Cloud environment, [create a symmetric GCP key ring and key](#).
2. Create a custom role for your Cloud Volumes ONTAP service account.

```
gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

  --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

3. Assign the custom role to the Cloud KMS key and Cloud Volumes ONTAP service account:

```
gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
--location key_location --member serviceAccount:_service_account_Name_ --role
projects/customer_project_id/roles/kmsCustomRole
```

4. Download service account JSON key:

```
gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com
```

#### Cloud Volumes ONTAP

1. Connect to the cluster management LIF with your preferred SSH client.
2. Switch to the advanced privilege level:  
`set -privilege advanced`
3. Create a DNS for the data SVM.  
`dns create -domains c.<project>.internal -name-servers server_address -vserver SVM_name`

#### 4. Create CMEK entry:

```
security key-manager external gcp enable -vserver SVM_name -project-id project  
-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name  
key_name
```

#### 5. When prompted, enter the service account JSON key from your GCP account.

#### 6. Confirm the enabled process succeeded:

```
security key-manager external gcp check -vserver svm_name
```

#### 7. OPTIONAL: Create a volume to test encryption

```
vol create volume_name -aggregate aggregate  
-vserver vservers_name -size 10G
```

## Troubleshoot

If you need to troubleshoot, you can tail the raw REST API logs in the final two steps above:

```
.set d  
.systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log
```

# System administration

## Upgrade Cloud Volumes ONTAP software

Upgrade Cloud Volumes ONTAP from Cloud Manager to gain access to the latest new features and enhancements. You should prepare Cloud Volumes ONTAP systems before you upgrade the software.

### Upgrade overview

You should be aware of the following before you start the Cloud Volumes ONTAP upgrade process.

#### Upgrade from Cloud Manager only

Upgrades of Cloud Volumes ONTAP must be completed from Cloud Manager. You should not upgrade Cloud Volumes ONTAP by using System Manager or the CLI. Doing so can impact system stability.

### How to upgrade

Cloud Manager provides two ways to upgrade Cloud Volumes ONTAP:

- By following upgrade notifications that appear in the working environment
- By placing the upgrade image at an HTTPS location and then providing Cloud Manager with the URL

### Supported upgrade paths

The version of Cloud Volumes ONTAP that you can upgrade to depends on the version of Cloud Volumes ONTAP that you're currently running.

Current version	Versions that you can directly upgrade to
9.10.1	9.11.0



Current version	Versions that you can directly upgrade to
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Note the following:

- The supported upgrade paths for Cloud Volumes ONTAP are different than they are for an on-premises ONTAP cluster.
- If you upgrade by following the upgrade notifications that appear in a working environment, Cloud Manager will prompt you to upgrade to a release that follows these supported upgrade paths.
- If you upgrade by placing an upgrade image at an HTTPS location, be sure to follow these supported upgrade paths.
- In some cases, you might need to upgrade a few times to reach your target release.

For example, if you're running version 9.8 and you want to upgrade to 9.10.1, you first need to upgrade to version 9.9.1 and then to 9.10.1.

### Reverting or downgrading

Reverting or downgrading Cloud Volumes ONTAP to a previous release is not supported.

### Support registration

Cloud Volumes ONTAP must be registered with NetApp support in order to upgrade the software using any of the methods described on this page. This applies to both PAYGO and BYOL. You'll need to [manually register PAYGO systems](#), while BYOL systems are registered by default.



A system that isn't registered for support will still receive the software update notifications that appear in Cloud Manager when a new version is available. But you will need to register the system before you can upgrade the software.

## Upgrades of the HA mediator

Cloud Manager also updates the mediator instance as needed during the Cloud Volumes ONTAP upgrade process.

### Prepare to upgrade

Before performing an upgrade, you must verify that your systems are ready and make any required configuration changes.

- [Plan for downtime](#)
- [Verify that automatic giveback is still enabled](#)
- [Suspend SnapMirror transfers](#)
- [Verify that aggregates are online](#)

#### Plan for downtime

When you upgrade a single-node system, the upgrade process takes the system offline for up to 25 minutes, during which I/O is interrupted.

Upgrading an HA pair is nondisruptive and I/O is uninterrupted. During this nondisruptive upgrade process, each node is upgraded in tandem to continue serving I/O to clients.

#### Verify that automatic giveback is still enabled

Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

[ONTAP 9 Documentation: Commands for configuring automatic giveback](#)

#### Suspend SnapMirror transfers

If a Cloud Volumes ONTAP system has active SnapMirror relationships, it is best to suspend transfers before you update the Cloud Volumes ONTAP software. Suspending the transfers prevents SnapMirror failures. You must suspend the transfers from the destination system.



Even though Cloud Backup uses an implementation of SnapMirror to create backup files (called SnapMirror Cloud), backups do not need to be suspended when a system is upgraded.

#### About this task

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

#### Steps

1. Log in to System Manager from the destination system.

You can log in to System Manager by pointing your web browser to the IP address of the cluster management LIF. You can find the IP address in the Cloud Volumes ONTAP working environment.



The computer from which you are accessing Cloud Manager must have a network connection to Cloud Volumes ONTAP. For example, you might need to log in to Cloud Manager from a jump host that's in your cloud provider network.

2. Click **Protection > Relationships**.
3. Select the relationship and click **Operations > Quiesce**.

#### Verify that aggregates are online

Aggregates for Cloud Volumes ONTAP must be online before you update the software. Aggregates should be online in most configurations, but if they are not, then you should bring them online.

#### About this task

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

#### Steps

1. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
2. Select an aggregate, click **Info**, and then verify that the state is online.

aggr1		
Aggregate Capacity:	88.57 GB	
-----		
Used Aggregate Capacity:	1.07 GB	
-----		
Volumes:	2	▼
-----		
AWS Disks:	1	▼
-----		
State:	online	

3. If the aggregate is offline, use System Manager to bring the aggregate online:
  - a. Click **Storage > Aggregates & Disks > Aggregates**.
  - b. Select the aggregate, and then click **More Actions > Status > Online**.

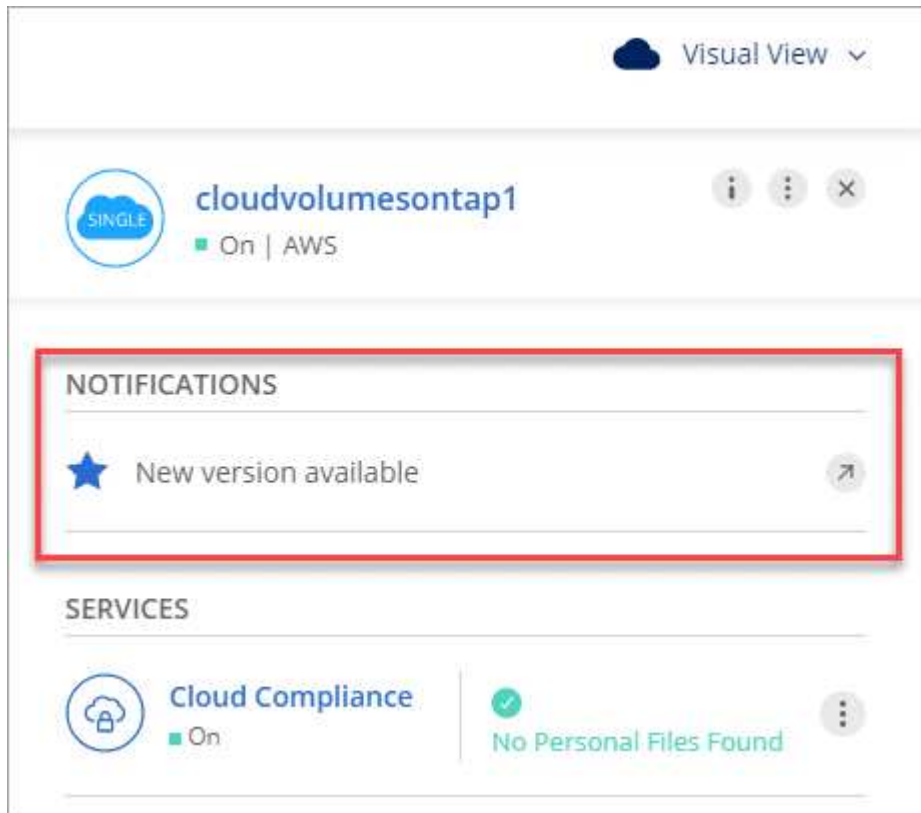
#### Upgrade Cloud Volumes ONTAP

Cloud Manager notifies you when a new version is available for upgrade. You can start the upgrade process from this notification. For details, see [Upgrade from Cloud Manager notifications](#).

Another way to perform software upgrades by using an image on an external URL. This option is helpful if Cloud Manager can't access the S3 bucket to upgrade the software or if you were provided with a patch. For details, see [Upgrade from an image available at a URL](#).

#### Upgrade from Cloud Manager notifications

Cloud Manager displays a notification in Cloud Volumes ONTAP working environments when a new version of Cloud Volumes ONTAP is available:



You can start the upgrade process from this notification, which automates the process by obtaining the software image from an S3 bucket, installing the image, and then restarting the system.

### Before you begin

Cloud Manager operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.

### Steps

1. Click **Canvas**.
2. Select a working environment.

A notification appears in the right pane if a new version is available:



3. If a new version is available, click **Upgrade**.
4. In the Release Information page, click the link to read the Release Notes for the specified version, and then select the **I have read...** check box.
5. In the End User License Agreement (EULA) page, read the EULA, and then select **I read and approve the EULA**.
6. In the Review and Approve page, read the important notes, select **I understand...**, and then click **Go**.

### Result

Cloud Manager starts the software upgrade. You can perform actions on the working environment once the software update is complete.

### After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

### Upgrade from an image available at a URL

You can place the Cloud Volumes ONTAP software image on the Connector or on an HTTP server and then initiate the software upgrade from Cloud Manager. You might use this option if Cloud Manager can't access the S3 bucket to upgrade the software.

### Before you begin

Cloud Manager operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.

### Steps

1. Optional: Set up an HTTP server that can host the Cloud Volumes ONTAP software image.

If you have a VPN connection to the virtual network, you can place the Cloud Volumes ONTAP software

image on an HTTP server in your own network. Otherwise, you must place the file on an HTTP server in the cloud.

2. If you use your own security group for Cloud Volumes ONTAP, ensure that the outbound rules allow HTTP connections so Cloud Volumes ONTAP can access the software image.



The predefined Cloud Volumes ONTAP security group allows outbound HTTP connections by default.

3. Obtain the software image from [the NetApp Support Site](#).
4. Copy the software image to a directory on the Connector or on an HTTP server from which the file will be served.

For example, you can copy the software image to the following path on the Connector:

```
/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/
```

5. From the working environment in Cloud Manager, click the menu icon, and then click **Advanced > Update Cloud Volumes ONTAP**.
6. On the update software page, enter the URL, and then click **Change Image**.

If you copied the software image to the Connector in the path shown above, you would enter the following URL:

```
http://<Connector-private-IP-address>/ontap/images/<image-file-name>
```

7. Click **Proceed** to confirm.

## Result

Cloud Manager starts the software update. You can perform actions on the working environment once the software update is complete.

## After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

## Fix download failures when using a Google Cloud NAT gateway

The Connector automatically downloads software updates for Cloud Volumes ONTAP. The download can fail if your configuration uses a Google Cloud NAT gateway. You can correct this issue by limiting the number of parts that the software image is divided into. This step must be completed by using the Cloud Manager API.

## Step

1. Submit a PUT request to `/occm/config` with the following JSON as body:

```
{
  "maxDownloadSessions": 32
}
```

The value for *maxDownloadSessions* can be 1 or any integer greater than 1. If the value is 1, then the downloaded image will not be divided.

Note that 32 is an example value. The value that you should use depends on your NAT configuration and the number of sessions that you can have simultaneously.

[Learn more about the /occm/config API call.](#)

## Registering pay-as-you-go systems

Support from NetApp is included with Cloud Volumes ONTAP PAYGO systems, but you must first activate support by registering the systems with NetApp.

Registering a PAYGO system with NetApp is required to upgrade ONTAP software using any of the methods [described on this page](#).



A system that isn't registered for support will still receive the software update notifications that appear in Cloud Manager when a new version is available. But you will need to register the system before you can upgrade the software.

### Steps

1. If you have not yet added your NetApp Support Site account to Cloud Manager, go to **Account Settings** and add it now.

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

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



4. Select a NetApp Support Site account and click **Register**.

### Result

Cloud Manager registers the system with NetApp.

## Managing the state of Cloud Volumes ONTAP

You can stop and start Cloud Volumes ONTAP from Cloud Manager to manage your cloud compute costs.

## Scheduling automatic shutdowns of Cloud Volumes ONTAP

You might want to shut down Cloud Volumes ONTAP during specific time intervals to lower your compute costs. Rather than do this manually, you can configure Cloud Manager to automatically shut down and then restart systems at specific times.

### About this task

- When you schedule an automatic shutdown of your Cloud Volumes ONTAP system, Cloud Manager postpones the shutdown if an active data transfer is in progress.

Cloud Manager shuts down the system after the transfer is complete.

- This task schedules automatic shutdowns of both nodes in an HA pair.
- Snapshots of boot and root disks are not created when turning off Cloud Volumes ONTAP through scheduled shutdowns.

Snapshots are automatically created only when performing a manual shutdown, as described in the next section.

### Steps

1. From the working environment, click the clock icon:



2. Specify the shutdown schedule:
  - a. Choose whether you want to shut down the system every day, every weekday, every weekend, or any combination of the three options.
  - b. Specify when you want to turn off the system and for how long you want it turned off.

### Example

The following image shows a schedule that instructs Cloud Manager to shut down the system every Saturday at 12:00 a.m. for 48 hours. Cloud Manager restarts the system every Monday at 12:00 a.m.

<input type="checkbox"/>	<b>Turn off every weekday</b> Mon, Tue, Wed, Thu, Fri	turn off at	08	:	00	PM	for	12	Hours (1-24)
<input checked="" type="checkbox"/>	<b>Turn off every weekend</b> Sat	turn off at	12	:	00	AM	for	48	Hours (1-48)

3. Click **Save**.

### Result

Cloud Manager saves the schedule. The clock icon changes to indicate that a schedule is set:



## Stopping Cloud Volumes ONTAP

Stopping Cloud Volumes ONTAP saves you from accruing compute costs and creates snapshots of the root and boot disks, which can be helpful for troubleshooting.



To reduce costs, Cloud Manager periodically deletes older snapshots of root and boot disks. Only the two most recent snapshots are retained for both the root and boot disks.

### About this task

When you stop an HA pair, Cloud Manager shuts down both nodes.

### Steps

1. From the working environment, click the **Turn off** icon.



2. Keep the option to create snapshots enabled because the snapshots can enable system recovery.
3. Click **Turn Off**.

It can take up to a few minutes to stop the system. You can restart systems at a later time from the working environment page.

## Synchronize the system time using NTP

Specifying an NTP server synchronizes the time between the systems in your network, which can help prevent issues due to time differences.

Specify an NTP server using the [Cloud Manager API](#) or from the user interface when you [create a CIFS server](#).

## Modify system write speed

Cloud Manager enables you to choose a normal or high write speed for Cloud Volumes ONTAP. The default write speed is normal. You can change to high write speed if fast write performance is required for your workload.

High write speed is supported with all types of single node systems and some HA pair configurations. View supported configurations in the [Cloud Volumes ONTAP Release Notes](#)

Before you change the write speed, you should [understand the differences between the normal and high settings](#).

### About this task

- Ensure that operations such as volume or aggregate creation are not in progress.
- Be aware that this change restarts the Cloud Volumes ONTAP system. This is disruptive process that requires downtime for the entire system.

### Steps

1. From the working environment, click the menu icon, and then click **Advanced > Writing Speed**.

2. Select **Normal** or **High**.

If you choose High, then you'll need to read the "I understand..." statement and confirm by checking the box.

3. Click **Save**, review the confirmation message, and then click **Proceed**.

## Change the password for Cloud Volumes ONTAP

Cloud Volumes ONTAP includes a cluster admin account. You can change the password for this account from Cloud Manager, if needed.



You should not change the password for the admin account through System Manager or the CLI. The password will not be reflected in Cloud Manager. As a result, Cloud Manager cannot monitor the instance properly.

### Steps

1. From the working environment, click the menu icon, and then click **Advanced > Set password**.
2. Enter the new password twice and then click **Save**.

The new password must be different than one of the last six passwords that you used.

## Add, remove, or delete systems

### Adding existing Cloud Volumes ONTAP systems to Cloud Manager

You can discover and add existing Cloud Volumes ONTAP systems to Cloud Manager. You might do this if you deployed a new Cloud Manager system.

### Before you begin

You must know the password for the Cloud Volumes ONTAP admin user account.

### Steps

1. On the Canvas page, click **Add Working Environment**.
2. Select the cloud provider in which the system resides.
3. Choose the type of Cloud Volumes ONTAP system.
4. Click the link to discover an existing system.



5. On the Region page, choose the region where the instances are running, and then select the instances.
6. On the Credentials page, enter the password for the Cloud Volumes ONTAP admin user, and then click **Go**.

### Result

Cloud Manager adds the Cloud Volumes ONTAP instances to the workspace.

### Removing Cloud Volumes ONTAP working environments

The Account Admin can remove a Cloud Volumes ONTAP working environment to move it to another system or to troubleshoot discovery issues.

#### About this task

Removing a Cloud Volumes ONTAP working environment removes it from Cloud Manager. It does not delete the Cloud Volumes ONTAP system. You can later rediscover the working environment.

Removing a working environment from Cloud Manager enables you to do the following:

- Rediscover it in another workspace
- Rediscover it from another Cloud Manager system
- Rediscover it if you had problems during the initial discovery

### Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Tools**.



2. From the Tools page, click **Launch**.
3. Select the Cloud Volumes ONTAP working environment that you want to remove.
4. On the Review and Approve page, click **Go**.

## Result

Cloud Manager removes the working environment. Users can rediscover this working environment from the Canvas page at any time.

## Deleting a Cloud Volumes ONTAP system

You should always delete Cloud Volumes ONTAP systems from Cloud Manager, rather than from your cloud provider's console. For example, if you terminate a licensed Cloud Volumes ONTAP instance from your cloud provider, then you can't use the license key for another instance. You must delete the working environment from Cloud Manager to release the license.

When you delete a working environment, Cloud Manager terminates Cloud Volumes ONTAP instances and deletes disks and snapshots.

Resources managed by other services like backups for Cloud Backup and instances for Cloud Data Sense and Monitoring are not deleted when you delete a working environment. You'll need to manually delete them yourself. If you don't, then you'll continue to receive charges for these resources.



When Cloud Manager deploys Cloud Volumes ONTAP in your cloud provider, it enables termination protection on the instances. This option helps prevent accidental termination.

## Steps

1. If you enabled Cloud Backup on the working environment, determine whether the backed up data is still required and then [delete the backups, if necessary](#).

Cloud Backup is independent from Cloud Volumes ONTAP by design. Cloud Backup doesn't automatically delete backups when you delete a Cloud Volumes ONTAP system, and there is no current support in the UI to delete the backups after the system has been deleted.

2. If you enabled Cloud Data Sense or Monitoring on this working environment and no other working environments use those services, then you'll need to delete the instances for those services.

- [Learn more about the Cloud Data Sense instance](#).
- [Learn more about the Monitoring Acquisition Unit](#).

3. Delete the Cloud Volumes ONTAP working environment.

- a. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment that you want to delete.
- b. Click menu icon and then click **Delete**.



c. Type the name of the working environment and then click **Delete**.

It can take up to 5 minutes to delete the working environment.

## Administration in AWS

### Change the EC2 instance type for Cloud Volumes ONTAP

You can choose from several instance or types when you launch Cloud Volumes ONTAP in AWS. You can change the instance type at any time if you determine that it is undersized or oversized for your needs.

#### About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

[ONTAP 9 Documentation: Commands for configuring automatic giveback](#)

- Changing the instance type can affect AWS service charges.
- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

For HA pairs, the change is nondisruptive. HA pairs continue to serve data.



Cloud Manager gracefully changes one node at a time by initiating takeover and waiting for give back. NetApp's QA team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, we did see retries on the I/O level, but the application layer overcame these short "re-wire" of NFS/CIFS connections.

### Steps

1. From the working environment, click the menu icon, and then select **Change instance**.
2. If you are using a node-based PAYGO license, you can optionally choose a different license.
3. Choose an instance type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

### Result

Cloud Volumes ONTAP reboots with the new configuration.

### Change route tables for HA pairs in multiple AZs

You can modify the AWS route tables that include routes to the floating IP addresses for an HA pair that's deployed in multiple AWS Availability Zones (AZs). You might do this if new NFS or CIFS clients need to access an HA pair in AWS.

### Steps

1. From the working environment, click the menu icon and then click **Information**.
2. Click **Route Tables**.
3. Modify the list of selected route tables and then click **Save**.

### Result

Cloud Manager sends an AWS request to modify the route tables.

### Monitoring AWS resource costs

Cloud Manager enables you to view the resource costs associated with running Cloud Volumes ONTAP in AWS. You can also see how much money you saved by using NetApp features that can reduce storage costs.

### About this task

Cloud Manager updates the costs when you refresh the page. You should refer to AWS for final cost details.

### Step

1. Verify that Cloud Manager can obtain cost information from AWS:
  - a. Ensure that the IAM policy that provides Cloud Manager with permissions includes the following actions:

```
"ce:GetReservationUtilization",  
"ce:GetDimensionValues",  
"ce:GetCostAndUsage",  
"ce:GetTags"
```

These actions are included in the latest [Cloud Manager policy](#). New systems deployed from NetApp Cloud Central automatically include these permissions.

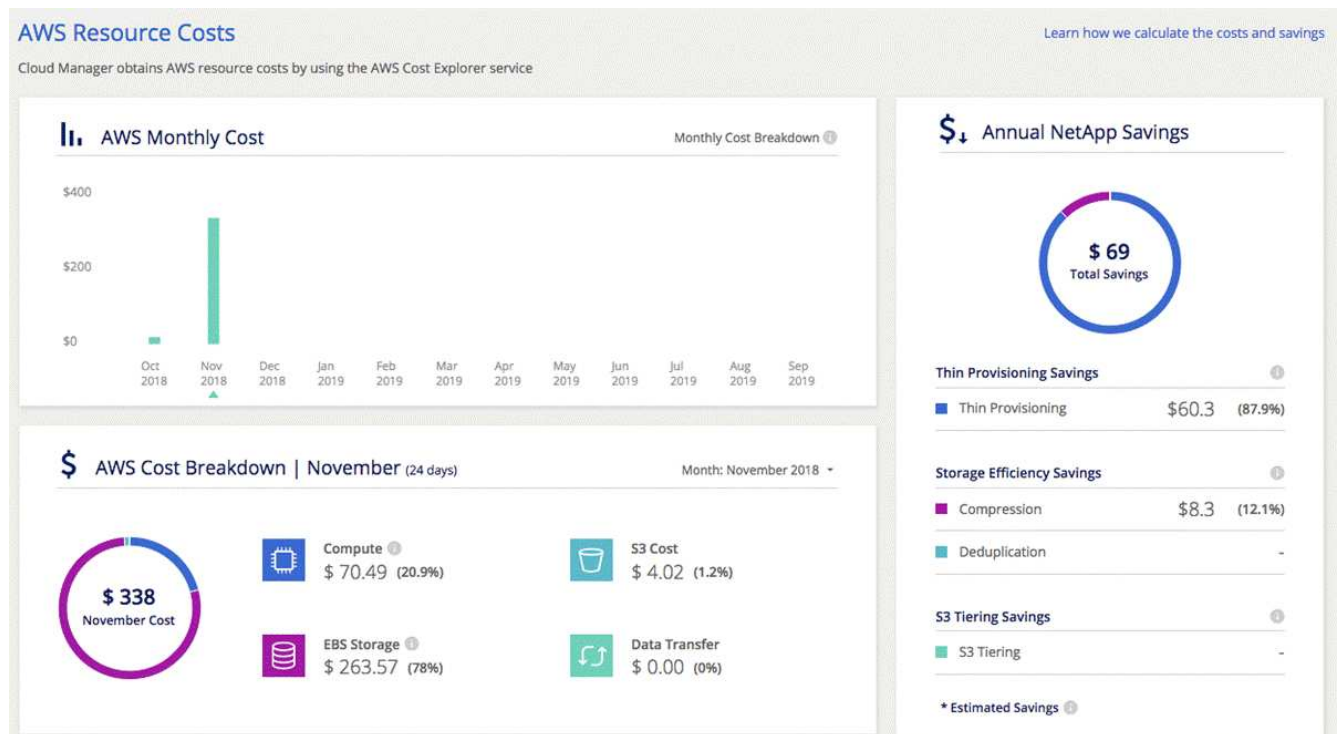
b. [Activate the WorkingEnvironmentId tag](#).

To track your AWS costs, Cloud Manager assigns a cost allocation tag to Cloud Volumes ONTAP instances. After you create your first working environment, activate the **WorkingEnvironmentId** tag. User-defined tags don't appear on AWS billing reports until you activate them in the Billing and Cost Management console.

2. On the Canvas page, select a Cloud Volumes ONTAP working environment and then click **Cost**.

The Cost page displays costs for the current and previous months and shows your annual NetApp savings, if you enabled NetApp's cost-saving features on volumes.

The following image shows a sample Cost page:



## Administration in Azure

### Change the Azure VM type for Cloud Volumes ONTAP

You can choose from several VM types when you launch Cloud Volumes ONTAP in Microsoft Azure. You can change the VM type at any time if you determine that it is undersized or oversized for your needs.

#### About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

[ONTAP 9 Documentation: Commands for configuring automatic giveback](#)



- Changing the VM type can affect Microsoft Azure service charges.
- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

For HA pairs, the change is nondisruptive. HA pairs continue to serve data.



Cloud Manager gracefully changes one node at a time by initiating takeover and waiting for give back. NetApp's QA team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, we did see retries on the I/O level, but the application layer overcame these short "re-wire" of NFS/CIFS connections.

## Steps

1. From the working environment, click the menu icon, and then select **Change VM**.
2. If you are using a node-based PAYGO license, you can optionally choose a different license.
3. Select a VM 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.

## Overriding CIFS locks for Cloud Volumes ONTAP HA pairs in Azure

The Account Admin can enable a setting in Cloud Manager that prevents issues with Cloud Volumes ONTAP storage giveback during Azure maintenance events. When you enable this setting, Cloud Volumes ONTAP vetoes CIFS locks and resets active CIFS sessions.

### About this task

Microsoft Azure schedules periodic maintenance events on its virtual machines. When a maintenance event occurs on a Cloud Volumes ONTAP HA pair, the HA pair initiates storage takeover. If there are active CIFS sessions during this maintenance event, the locks on CIFS files can prevent storage giveback.

If you enable this setting, Cloud Volumes ONTAP will veto the locks and reset the active CIFS sessions. As a result, the HA pair can complete storage giveback during these maintenance events.



This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

## What you'll need

You need to create a Connector before you can change Cloud Manager settings. [Learn how.](#)

## Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.





2. Under **Azure**, click **Azure CIFS locks for Azure HA working environments**.
3. Click the checkbox to enable the feature and then click **Save**.

### Using an Azure Private Link with Cloud Volumes ONTAP

By default, Cloud Manager enables an Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts. A Private Link secures connections between endpoints in Azure and provides performance benefits. [Learn more](#).

In most cases, there's nothing that you need to do—Cloud Manager manages the Azure Private Link for you. But if you use Azure Private DNS, then you'll need to edit a configuration file. You can also disable the Private Link connection, if desired.

#### Connector location in Azure

The Connector should be deployed in the same Azure region as the Cloud Volumes ONTAP systems that it manages, or in the [Azure region pair](#) for the Cloud Volumes ONTAP systems. This requirement ensures that an Azure Private Link connection is used between Cloud Volumes ONTAP and its associated storage accounts. [Learn how Cloud Volumes ONTAP uses an Azure Private Link](#).

#### How Private Link connections work with Cloud Volumes ONTAP

When Cloud Manager deploys Cloud Volumes ONTAP in Azure, it creates a private endpoint in the resource group. The private endpoint is associated with the storage account for Cloud Volumes ONTAP. As a result, access to Cloud Volumes ONTAP storage travels through the Microsoft backbone network.

Client access goes through the private link when clients are within the same VNet as Cloud Volumes ONTAP, within peered VNets, or in your on-premises network when using a private VPN or ExpressRoute connection to the VNet.

Here's an example that shows client access over a private link from within the same VNet and from an on-prem network that has either a private VPN or ExpressRoute connection.



### Provide Cloud Manager with details about your Azure Private DNS

If you use [Azure Private DNS](#), then you need to modify a configuration file on each Connector. Otherwise, Cloud Manager can't enable the Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts.

Note that the DNS name must match Azure DNS naming requirements [as shown in Azure documentation](#).

### Steps

1. SSH to the Connector host and log in.
2. Navigate to the following directory: `/opt/application/netapp/cloudmanager/docker_occm/data`
3. Edit `app.conf` by modifying the following parameters as shown:

```
"user-private-dns-zone-settings": {
  "use-existing": true,
  "resource-group": "<resource group name of the DNS zone>",
  "subscription": "<subscription ID>"
}
```

The subscription parameter is required only if the Private DNS Zone exists in a different subscription than

the Connector.

4. Save the file and log off the Connector.

A reboot isn't required.

### Enable rollback on failures

If Cloud Manager fails to create an Azure Private Link as part of specific actions, it completes the action without the Azure Private Link connection. This can happen when creating a new working environment (single node or HA pair), or when the following actions occur on an HA pair: creating a new aggregate, adding disks to an existing aggregate, or creating a new storage account when going above 32 TiB.

You can change this default behavior by enabling rollback if Cloud Manager fails to create the Azure Private Link. This can help to ensure that you're fully compliant with your company's security regulations.

If you enable rollback, Cloud Manager stops the action and rolls back all resources that were created as part of the action.

Enabling rollback is supported through the API only.

### Step

1. Use the `PUT /occm/config` API call with the following request body:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

### Disable Azure Private Link connections

If required for your Azure configuration, you can disable the Azure Private Link connection between Cloud Volumes ONTAP and storage accounts.

### Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.
2. Under **Azure**, click **Use Azure Private Link**.
3. Deselect **Private Link connection between Cloud Volumes ONTAP and storage accounts**.
4. Click **Save**.

## Administration in Google Cloud

### Change the Google Cloud machine type for Cloud Volumes ONTAP

You can choose from several machine types when you launch Cloud Volumes ONTAP in Google Cloud. You can change the instance or machine type at any time if you determine that it is undersized or oversized for your needs.

### About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

- Changing the machine type can affect Google Cloud service charges.
- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

For HA pairs, the change is nondisruptive. HA pairs continue to serve data.



Cloud Manager gracefully changes one node at a time by initiating takeover and waiting for give back. NetApp's QA team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, we did see retries on the I/O level, but the application layer overcame these short "re-wire" of NFS/CIFS connections.

### Steps

1. From the working environment, click the menu icon, and then select **Change machine**.
2. If you are using a node-based PAYGO license, you can optionally choose a different license.
3. Select a 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.

## Use System Manager or the CLI

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using ONTAP System Manager or the command line interface.

### Connecting to System Manager

You might need to perform some Cloud Volumes ONTAP tasks from System Manager, which is a browser-based management tool that runs on the Cloud Volumes ONTAP system. For example, you need to use System Manager if you want to create LUNs.

### Before you begin

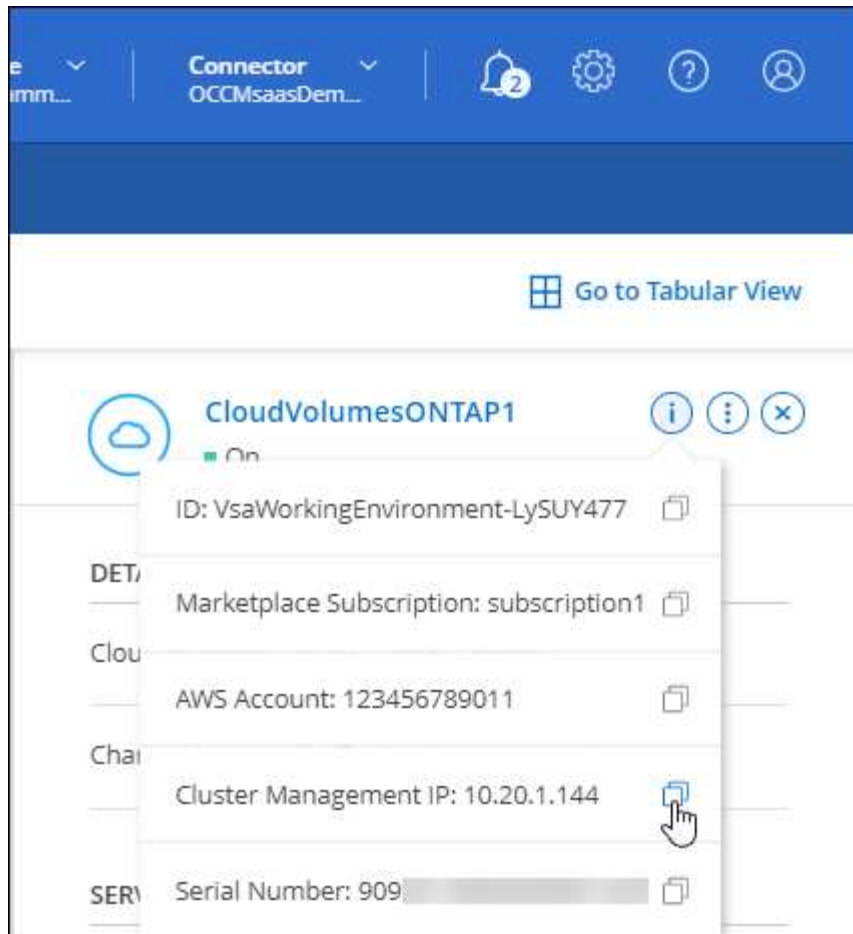
The computer from which you are accessing Cloud Manager must have a network connection to Cloud Volumes ONTAP. For example, you might need to log in to Cloud Manager from a jump host that's in your cloud provider network.



When deployed in multiple AWS Availability Zones, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

### Steps

1. From the Canvas, select the Cloud Volumes ONTAP working environment.
2. On the right pane, click the information icon and copy the cluster management IP.



3. Open a web browser on the machine that has a network connection to Cloud Volumes ONTAP and enter the IP address.
4. At the login screen, enter **admin** in the User Name field, enter the password that you specified when you created the working environment, and then click **Sign In**.

### Result

The System Manager console loads. You can now use it to manage Cloud Volumes ONTAP.

### Connecting to the Cloud Volumes ONTAP CLI

The Cloud Volumes ONTAP CLI enables you to run all administrative commands and is a good choice for advanced tasks or if you are more comfortable using the CLI. You can connect to the CLI using Secure Shell (SSH).

#### Before you begin

The host from which you use SSH to connect to Cloud Volumes ONTAP must have a network connection to Cloud Volumes ONTAP. For example, you might need to SSH from a jump host that's in your cloud provider network.



When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

### Steps

1. In Cloud Manager, identify the IP address of the cluster management interface:
  - a. On the Canvas page, select the Cloud Volumes ONTAP system.
  - b. Copy the cluster management IP address that appears in the right pane.
2. Use SSH to connect to the cluster management interface IP address using the admin account.

### Example

The following image shows an example using PuTTY:



3. At the login prompt, enter the password for the admin account.

### Example

```
Password: *****  
COT2::>
```

## System health and events

### Verify AutoSupport setup

AutoSupport proactively monitors the health of your system and sends messages to NetApp technical support. By default, AutoSupport is enabled on each node to send messages to technical support using the HTTPS transport protocol. It's best to verify that AutoSupport can send these messages.

If the Cloud Manager Account Admin added a proxy server to Cloud Manager before you launched your instance, Cloud Volumes ONTAP is configured to use that proxy server for AutoSupport messages.

The only required configuration step is to ensure that Cloud Volumes ONTAP has outbound internet connectivity through a NAT instance or your environment's proxy services. For details, refer to the networking requirements for your cloud provider.

- [AWS networking requirements](#)
- [Azure networking requirement](#)
- [Google Cloud networking requirements](#)

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

## Configure EMS

The Event Management System (EMS) collects and displays information about events that occur on ONTAP systems. To receive event notifications, you can set event destinations (email addresses, SNMP trap hosts, or syslog servers) and event routes for a particular event severity.

You can configure EMS using the CLI. For instructions, refer to [ONTAP docs: EMS configuration overview](#).

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.