



Provision and manage storage

Cloud Manager

NetApp

June 15, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_provisioning_storage.html on June 15, 2020. Always check docs.netapp.com for the latest.

Table of Contents

- Provision and manage storage 1
 - Provisioning storage 1
 - Managing existing storage 6
 - Tiering inactive data to low-cost object storage 14
 - Using ONTAP as persistent storage for Kubernetes 18
 - Encrypting volumes with NetApp encryption solutions 20

Provision and manage storage

Provisioning storage

You can provision additional storage for your Cloud Volumes ONTAP systems from Cloud Manager by managing volumes and aggregates.



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.

Creating FlexVol volumes

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

Before you begin

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

Steps

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

Action	Steps
Create a new volume and let Cloud Manager choose the containing aggregate	Click Add New Volume .
Create a new volume on a specific aggregate	<div>a. Click the menu icon, and then click Advanced > Advanced allocation.</div> <div>b. Click the menu for an aggregate.</div> <div>c. Click Create volume.</div>

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

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

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

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

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

Field	Description
Organizational Unit	<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"> • To configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter OU=Computers,OU=corp in this field. • To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter OU=AADDC Computers or OU=AADDC Users in this field. <p>Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</p>
DNS Domain	<p>The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.</p>
NTP Server	<p>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 API Developer Guide for details.</p>

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

For help, refer to the following:

- [Understanding volume usage profiles](#)
- [Sizing your system in AWS](#)
- [Sizing your system in Azure](#)
- [Data tiering overview](#)

6. Click **Go**.

Result

Cloud Volumes ONTAP provisions the volume.

After you finish

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

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

Creating FlexVol volumes on the second node in an HA configuration

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

Steps

1. On the Working Environments 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**.

After you finish

You can create additional volumes on this aggregate if required.



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.

Creating aggregates

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

Steps

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

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

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

Provisioning iSCSI LUNs

Create iSCSI LUNs by using a Cloud Manager API or by going to System Manager.

If you want to use the Cloud Manager APIs, [view an example here](#).

If you want to use System Manager, follow the steps below.

Before you begin

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

About this task

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

Steps

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

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

Using FlexCache volumes to accelerate data access

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 GB usage limit.



To generate the license, Cloud Manager needs to access <https://ipa-signer.cloudmanager.netapp.com>. Make sure that this URL is accessible from your firewall.



Managing existing storage

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



Managing existing volumes


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

Steps

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

Task	Action
View information about a volume	Select a volume, and then click Info .

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

Task	Action
Change the tiering policy	<ol style="list-style-type: none"> Select a volume, and then click Change Disk Type & Tiering Policy. Click Edit Policy. Select a different policy and click Change. <div>  <p>Cloud Manager moves the volume to an existing aggregate that uses the selected disk type with tiering, or it creates a new aggregate for the volume.</p> </div>
Delete a volume	<ol style="list-style-type: none"> Select a volume, and then click Delete. Click Delete again to confirm.

Managing existing aggregates

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

Before you begin

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


About this task

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

Steps

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

Task	Action
View information about an aggregate	Select an aggregate and click Info .
Create a volume on a specific aggregate	Select an aggregate and click Create volume .

Task	Action
Add disks to an aggregate	<p>a. Select an aggregate and click Add AWS disks or Add Azure disks.</p> <p>b. Select the number of disks that you want to add and click Add.</p> <div>  <div>All disks in an aggregate must be the same size.</div> </div>
Delete an aggregate	<p>a. Select an aggregate that does not contain any volumes and click Delete.</p> <p>b. Click Delete again to confirm.</p>

Modifying the CIFS server

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

Steps

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>
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	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <p>If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter OU=Computers,OU=corp in this field.</p>

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.
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 API Developer Guide for details.

3. Click **Save**.

Result

Cloud Volumes ONTAP updates the CIFS server with the changes.

Moving 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](#).

Moving 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 it cannot provide recommendations to correct the issue. If this happens, you need to identify how to correct the issue and then move one or more volumes.

Steps

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

Identifying how to correct capacity issues

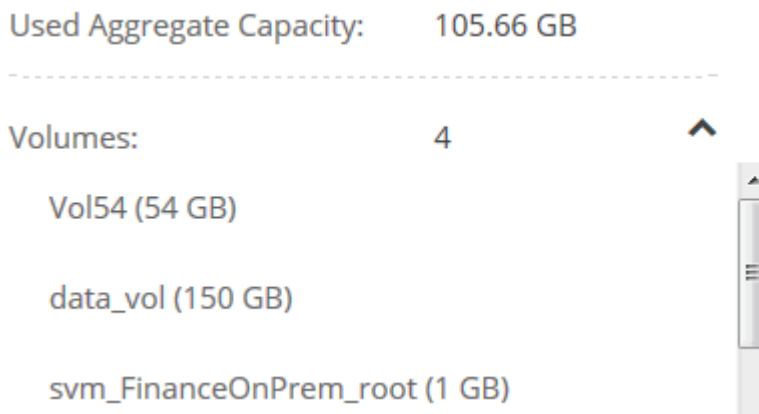
If Cloud Manager cannot provide recommendations for moving a volume to avoid capacity issues, you must identify the volumes that you need to move and whether you should move them to another aggregate on the same system or to another system.

Steps

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

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

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



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

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

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

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

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

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

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

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

Moving volumes to another system to avoid capacity issues

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

About this task

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

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

Steps

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

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

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

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

4. Configure the volume for data access.

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

5. Delete the original volume.

For details, see [Managing existing volumes](#).

Moving volumes to another aggregate to avoid capacity issues

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

About this task

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

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

Steps

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

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.
- The Cloud Volumes ONTAP system is in AWS and one aggregate 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 by combining an SSD or HDD performance tier for hot data with an object storage capacity tier for inactive data. For a high-level overview, see [Data tiering overview](#).

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



Choose a supported configuration

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



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 GCP, you need to configure the subnet for Private Google Access and set up a service account. [Learn more](#).



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 the capacity tier (an S3 bucket, Azure Blob container, or GCP bucket). Cloud Manager does that for you.

Configurations that support data tiering

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

- Data tiering is supported with Cloud Volumes ONTAP Standard, Premium, and BYOL, starting with the following versions:
 - Version 9.2 in AWS
 - Version 9.4 in Azure with single node systems
 - Version 9.6 in Azure with HA pairs
 - Version 9.6 in GCP



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

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

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](#).
- Cloud Volumes ONTAP 9.7: You need to create a service account that has the predefined Storage Admin role. You'll need to select this service account when you create a Cloud Volumes ONTAP working environment. For more details, see step 3 in [Getting started with Cloud Volumes ONTAP in Google Cloud Platform](#).

If you don't enable data tiering and select a service account when you create the Cloud Volumes ONTAP 9.7 system, then you'll need to turn off the system and add the service account to Cloud Volumes ONTAP from the GCP console.

- Cloud Volumes ONTAP 9.6: You need to add a Google Cloud Platform account to Cloud Manager by entering storage access keys for a service account. The keys enable Cloud Manager to set up a Cloud Storage bucket for data tiering. For instructions, see [Setting up and adding GCP accounts for data tiering with 9.6](#).

Tiering data from read-write volumes

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

Steps

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

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

2. Select the Snapshot Only policy or the Auto policy.

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

Example



Tiering data to object storage

Volume Tiering Policy

- ☒ **Auto** - Tiers cold Snapshot copies and cold user data from the active file system to object storage.
- ☐ **Snapshot Only** - Tiers cold Snapshot copies to object storage
- ☐ **None** - Data tiering is disabled.

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



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

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

Example



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**.

Using ONTAP as persistent storage for Kubernetes

Cloud Manager can automate the deployment of [NetApp Trident](#) on Kubernetes clusters so you can use ONTAP as persistent storage for containers. This works with Cloud Volumes ONTAP and on-prem ONTAP clusters.

Before you complete these steps, you need to [create a Cloud Volumes ONTAP system](#) or [discover an on-premises ONTAP cluster](#) from Cloud Manager.



Verify network connectivity

- a. A network connection must be available between Cloud Manager and the Kubernetes clusters, and from the Kubernetes clusters to ONTAP systems.
- b. Cloud Manager needs an outbound internet connection to access the following endpoints when installing Trident:

<https://packages.cloud.google.com/yum>

<https://github.com/NetApp/trident/releases/download/>

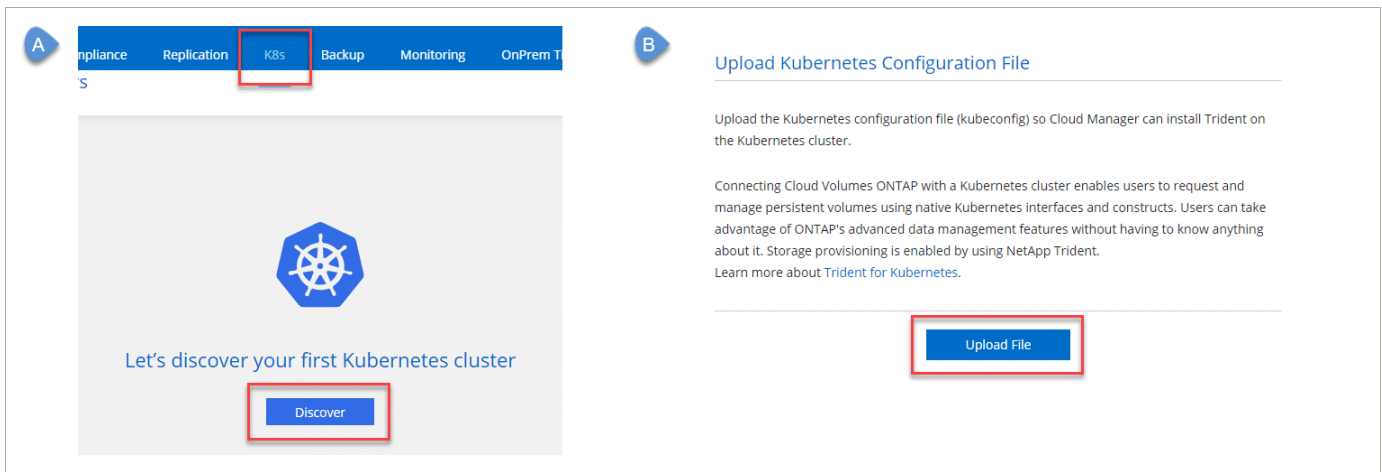
Cloud Manager installs Trident on a Kubernetes cluster when you connect a working environment to the cluster.



Upload Kubernetes configuration files to Cloud Manager

For each Kubernetes cluster, the Account Admin needs to upload a configuration file (kubeconfig) that is in YAML format. After you upload the file, Cloud Manager verifies connectivity to the cluster and saves an encrypted copy of the kubeconfig file.

Click **K8s > Discover > Upload File** and select the kubeconfig file.

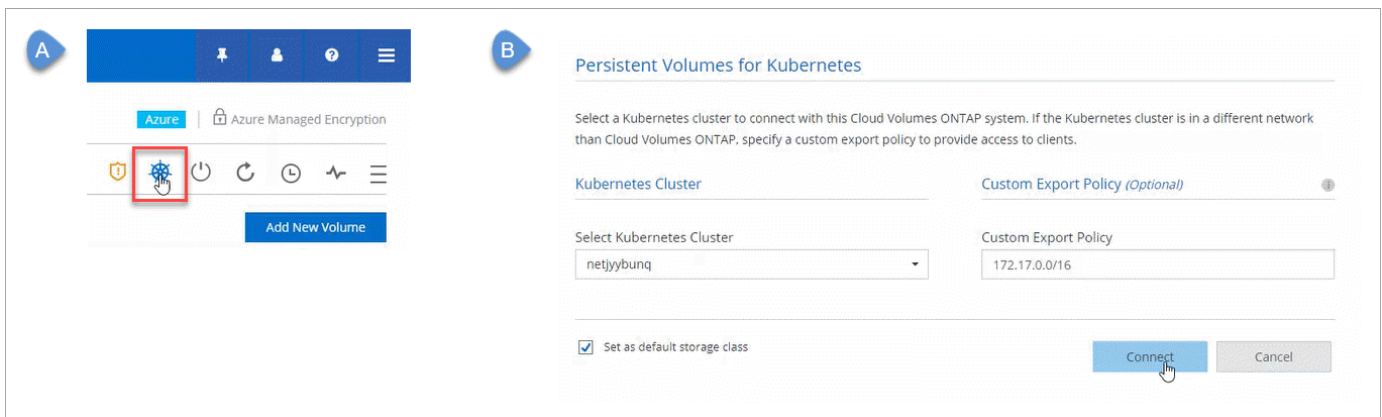


3

Connect your working environments to Kubernetes clusters

From the working environment, click the Kubernetes icon and follow the prompts. You can connect different clusters to different ONTAP systems and multiple clusters to the same ONTAP system.

You have the option to set the NetApp storage class as the default storage class for the Kubernetes cluster. When a user creates a persistent volume, the Kubernetes cluster can use connected ONTAP systems as the backend storage by default.



4

Start provisioning Persistent Volumes

Request and manage Persistent Volumes using native Kubernetes interfaces and constructs. Cloud Manager creates four Kubernetes storage classes that you can use when provisioning Persistent Volumes:

- **netapp-file**: for binding Persistent Volumes to single-node ONTAP systems
- **netapp-file-san**: for binding iSCSI Persistent Volumes to single-node ONTAP systems
- **netapp-file-redundant**: for binding Persistent Volumes to ONTAP HA pairs
- **netapp-file-redundant-san**: for binding iSCSI Persistent Volumes to ONTAP HA pairs

Cloud Manager configures Trident to use the following provisioning options by default:

- Thin volumes
- The default Snapshot policy
- Accessible Snapshot directory

[Learn more about provisioning your first volume with Trident for Kubernetes](#)

What are the trident_trident volumes?

Cloud Manager creates a volume on the first ONTAP system that you connect to a Kubernetes cluster. The name of the volume is appended with "_trident_trident." ONTAP uses this volume to connect to the Kubernetes cluster. You should not delete these volumes.

What happens when you disconnect or remove a Kubernetes cluster?

Cloud Manager enables you to disconnect individual ONTAP systems from a Kubernetes cluster. When you disconnect a system, you can no longer use that ONTAP system as persistent storage for containers. Existing Persistent Volumes are not deleted.

After you disconnect all systems from a Kubernetes cluster, you can also remove the entire Kubernetes configuration from Cloud Manager. Cloud Manager does not uninstall Trident when you remove the cluster and it does not delete any Persistent Volumes.

Both of these actions are available through APIs only. We plan to add the actions to the interface in a future release.

[Click here for details about the APIs.](#)

Encrypting volumes with NetApp encryption solutions

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

Starting with Cloud Volumes ONTAP 9.7, 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. Starting with Cloud Manager 3.7.1, 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. Install SSL certificates and connect to the external key management servers.

[ONTAP 9 NetApp Encryption Power Guide: Configuring external key management](#)

Copyright Information

Copyright © 2020 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.