NetApp

Provision and manage storage

Cloud Manager

NetApp
February 28, 2021

Table of Contents

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, CIFS, or iSCSI from Cloud Manager.

About this task

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.

> ℹ️ You can create additional LUNs from System Manager or the CLI.

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

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

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

Field	Description
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. • 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. Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain
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.

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 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**.

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 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**.

Connecting 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:

1. Cloud Manager's automatic capacity management doesn't apply to LUNs. When Cloud Manager creates a LUN, it disables the autogrow feature.

2. 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

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.

> **ℹ** 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 Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.

2. Manage your volumes:

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

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

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

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

3. Manage your aggregates:

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

Task	Action
Create a volume on a specific aggregate	Select an aggregate and click **Create volume**.
Add disks to an aggregate	a. Select an aggregate and click **Add AWS disks** or **Add Azure disks**. b. Select the number of disks that you want to add and click **Add**. All disks in an aggregate must be the same size.
Delete an aggregate	a. Select an aggregate that does not contain any volumes and click **Delete**. b. Click **Delete** again to confirm.

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

Task	Action
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.

   Used Aggregate Capacity: 105.66 GB

   Volumes: 4   ^

      Vol54 (54 GB)

      data_vol (150 GB)

      svm_FinanceOnPrem_root (1 GB)
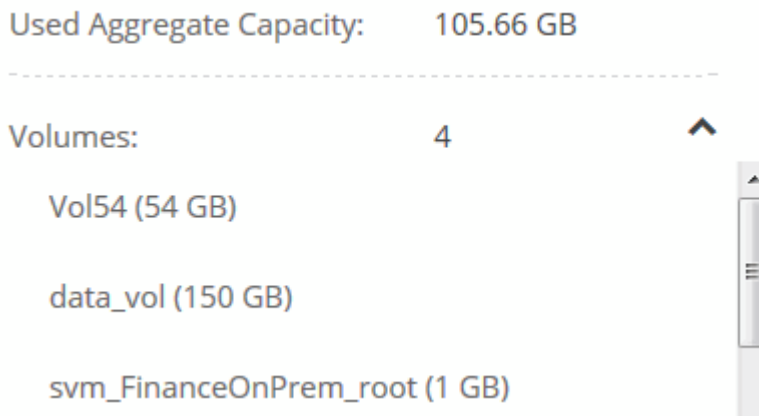
   d. Review the size of each volume and choose one or more volumes to move out of the aggregate.

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

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

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

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

   a. Delete any unused volumes.

   b. Rearrange volumes to free space on an aggregate.

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

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

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

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 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 Standard, Premium, or BYOL 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 GCP, 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 the capacity tier (an S3 bucket, Azure Blob container, or GCP bucket). 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:

- 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

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.

    Read step-by-step instructions.

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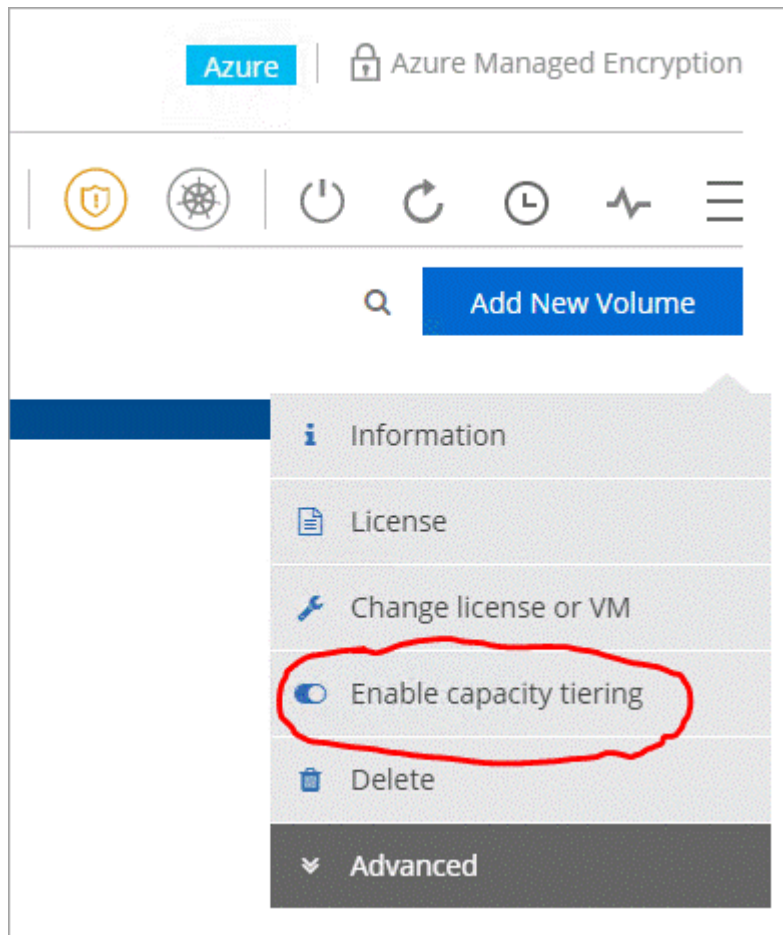
> ℹ️ You'll only see this option if data tiering couldn't be enabled when Cloud Manager created the system.

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.
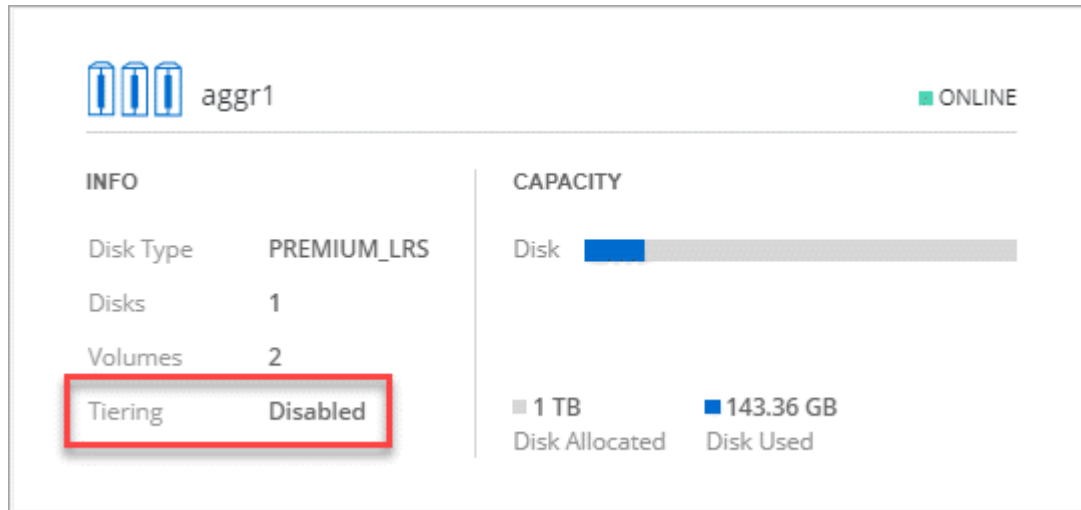
Steps to enable tiering on an aggregate

1. In System Manager, click **Storage > Tiers**.

2. Click the action menu for the aggregate and select **Attach Cloud Tiers**.

3. Select the cloud tier to attach and click **Save**.

What's next?

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

Tiering data from read-write volumes

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

Steps

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

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

2. Select a tiering policy.

   For a description of these policies, see Data tiering overview.

   Example

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

Tiering data from data protection volumes

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

Steps

1. On the Canvas page, select the working environment that contains the source volume, and then drag it to the working environment to which you want to replicate the volume.

2. Follow the prompts until you reach the tiering page and enable data tiering to object storage.

Example

For help with replicating data, see Replicating data to and from the cloud.

Changing the storage class for tiered data

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

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

For information about supported storage classes, see Data tiering overview.

Steps

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**.

Manage storage VMs

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
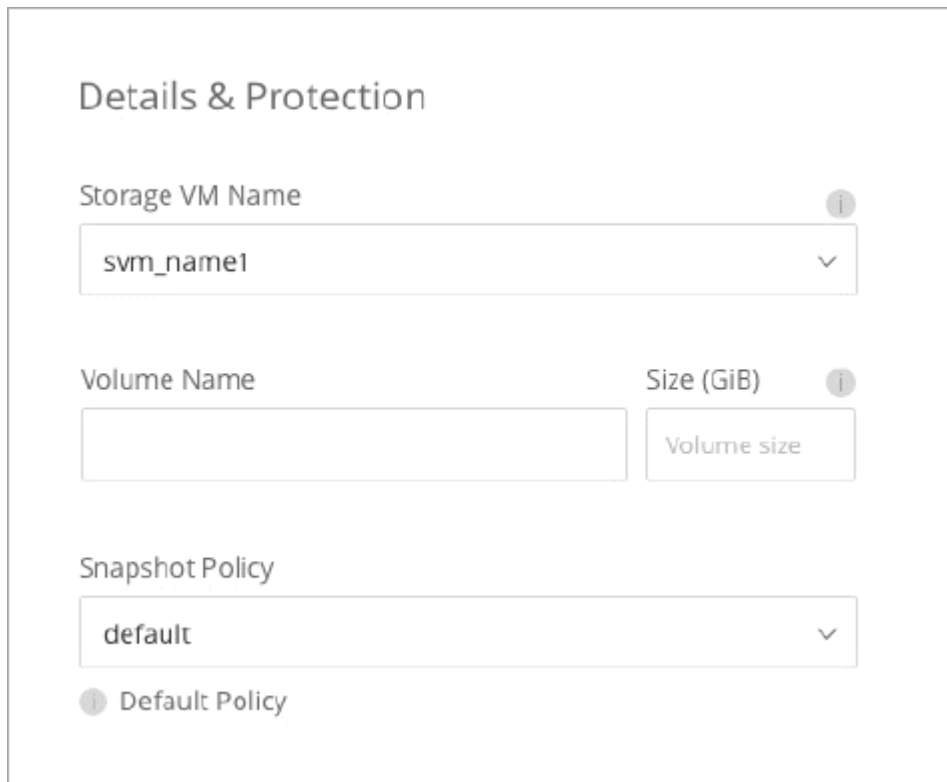
Cloud Volumes ONTAP 9.7 and 9.8 support multiple storage VMs in AWS with certain configurations and an add-on license. View the number of supported storage VMs in AWS. Contact your account team to obtain an SVM add-on license.

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.

Work with storage VMs in Cloud Manager

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

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

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

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

As noted above, multiple storage VMs are supported with Cloud Volumes ONTAP in AWS. To create additional storage VMs, you need to allocate IP addresses in AWS and then run ONTAP commands based on your Cloud Volumes ONTAP configuration.

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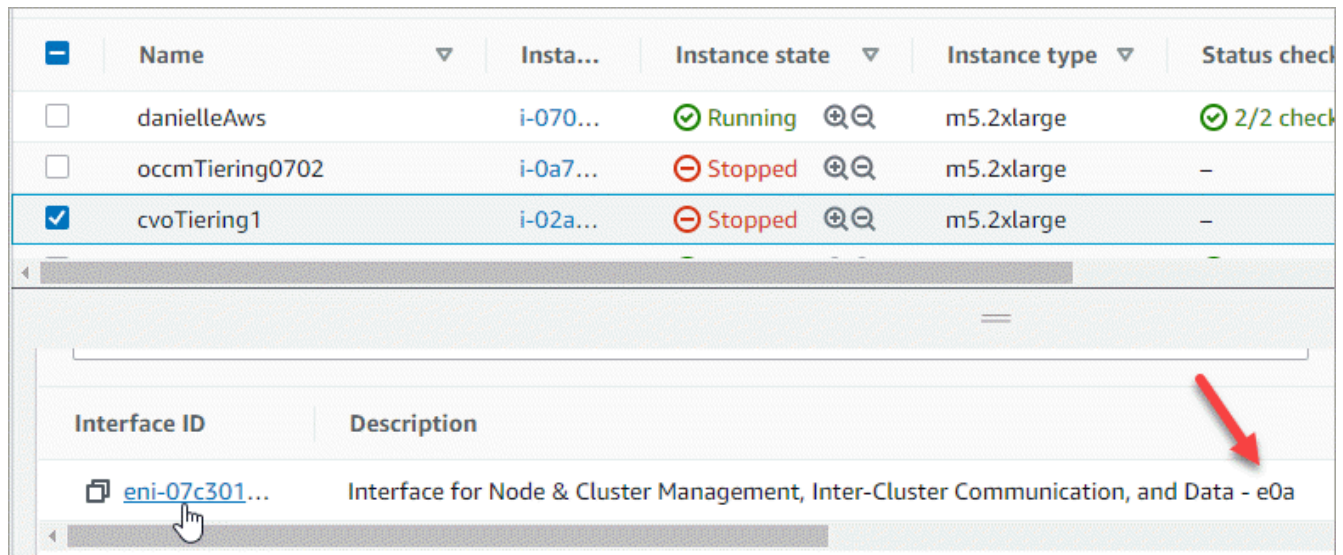
Note that an optional management LIF for a storage VM requires a private IP address on a single node system and on an HA pair in a single AZ. This management LIF provides a connection to management tools like SnapCenter.

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 mixed -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.

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 mixed -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.

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 mixed -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

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

2. Create a NAS LIF on node 1.

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

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

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

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

4. Create an iSCSI LIF on node 1.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

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

5. Create an iSCSI LIF on node 2.

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

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

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.

Using Cloud Volumes ONTAP as persistent storage for Kubernetes

Cloud Manager can automate the deployment of NetApp Trident on Kubernetes clusters so you can use Cloud Volumes ONTAP as persistent storage for containers.

Trident is a fully-supported open source project maintained by NetApp. Trident integrates natively with Kubernetes and its Persistent Volume framework to seamlessly provision and manage volumes from systems running any combination of NetApp's storage platforms. Learn more about Trident.

> **ⓘ** The Kubernetes feature isn't supported with on-prem ONTAP clusters. It's supported with Cloud Volumes ONTAP only.

Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

① Review prerequisites

Ensure that your environment can meet the prerequisites, which includes connectivity between Kubernetes clusters and Cloud Volumes ONTAP, connectivity between Kubernetes clusters and a Connector, a minimum Kubernetes version of 1.14, at least one worker node in a cluster, and more. See the complete list.

② Add your Kubernetes clusters to Cloud Manager

In Cloud Manager, click **K8s** and discover clusters directly from your cloud provider's managed service or import a cluster by providing a kubeconfig file.

③ Connect your clusters to Cloud Volumes ONTAP

After you add a Kubernetes cluster, click **Connect to Working Environment** to connect the cluster to one or more Cloud Volumes ONTAP systems.

④ Start provisioning Persistent Volumes

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

Learn more about provisioning your first volume with Trident for Kubernetes.

Reviewing prerequisites

Before you get started, ensure that your Kubernetes clusters and Connector meet specific requirements.

Kubernetes cluster requirements

- Network connectivity is required between a Kubernetes cluster and the Connector and between a Kubernetes cluster and Cloud Volumes ONTAP.

  Both the Connector and Cloud Volumes ONTAP need a connection to the Kubernetes API endpoint:

  ◦ For managed clusters, set up a route between a cluster's VPC and the VPC where the Connector and Cloud Volumes ONTAP reside.

  ◦ For other clusters, the IP address of the master node or load balancer (as listed in the kubeconfig file) must be reachable by the Connector and Cloud Volumes ONTAP, and it must present a valid TLS certificate.

- A Kubernetes cluster can be in any location that has the network connectivity listed above.

- A Kubernetes cluster must be running version 1.14 at a minimum.

  The maximum supported version is defined by Trident. Click here to see the maximum supported Kubernetes version.

- A Kubernetes cluster must have at least one worker node.

- For clusters running in Amazon Elastic Kubernetes Service (Amazon EKS), each cluster needs an IAM role added in order to resolve a permissions error. After you add the cluster, Cloud Manager will prompt you with the exact eksctl command that resolves the error.

  Learn about IAM permissions boundaries.

- For clusters running in Azure Kubernetes Service (AKS), those clusters must be assigned the *Azure Kubernetes Service RBAC Cluster Admin* role. This is required so Cloud Manager can install Trident and configure storage classes on the cluster.

- For clusters running in Google Kubernetes Engine (GKE), those clusters must not use the default Container Optimized OS. You should switch them to use Ubuntu.

  GKE defaults to using the Google container-optimized image, which doesn't have the utilities that Trident needs to mount volumes.

Connector requirements

Ensure that the following permissions are in place for the Connector.

Required permissions to discover and manage EKS clusters

The Connector needs Admin permissions to discover and manage Kubernetes clusters running in Amazon Elastic Kubernetes Service (EKS):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "eks:*",
            "Resource": "*"
        }
    ]
}
```

Required permissions to discover and manage GKE clusters

The Connector needs the following permissions to discover and manage Kubernetes clusters running in Google Kubernetes Engine (GKE):

```
container.*
```

Example setup

The following image shows an example of a Kubernetes cluster running in Amazon Elastic Kubernetes Service (Amazon EKS) and its connections to the Connector and Cloud Volumes ONTAP.
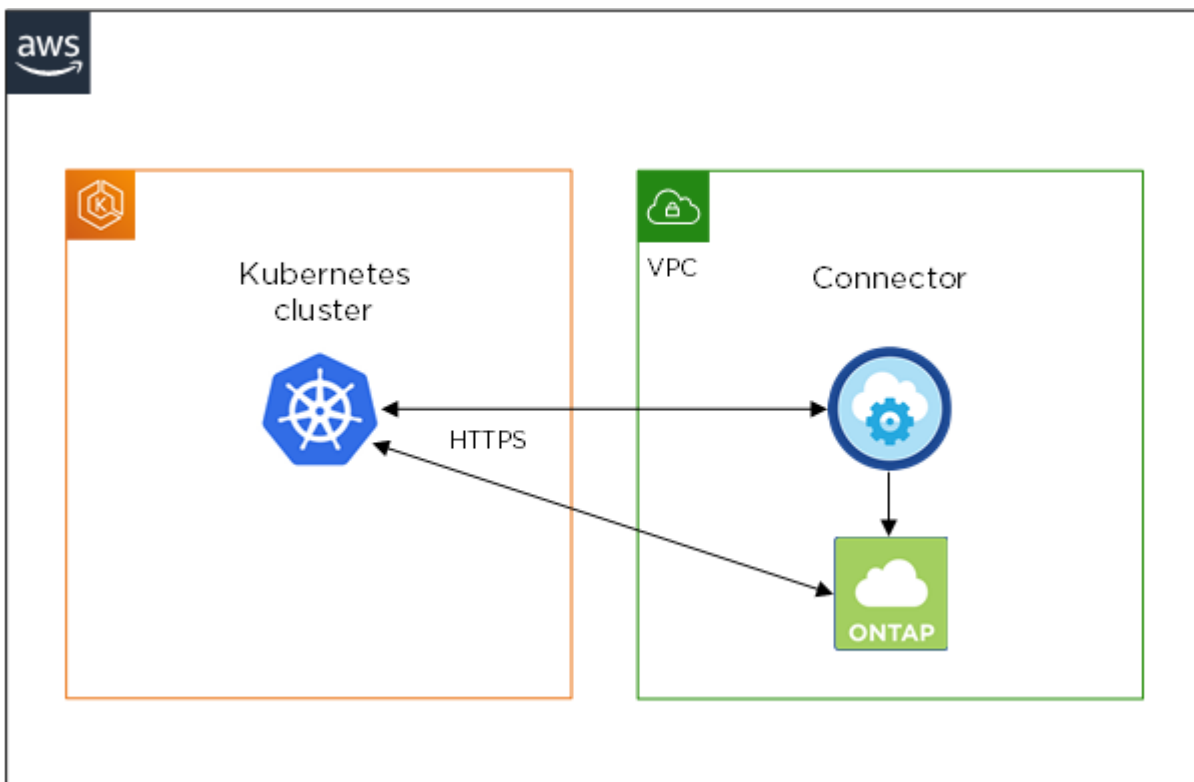
Adding Kubernetes clusters

Add Kubernetes clusters to Cloud Manager by discovering the clusters running in your cloud provider's managed Kubernetes service or by importing a cluster's kubeconfig file.

Steps

1. At the top of Cloud Manager, click **K8s**.

2. Click **Add Cluster**.

3. Choose one of the available options:

   ◦ Click **Discover Clusters** to discover the managed clusters that Cloud Manager has access to based on permissions that you provided to the Connector.

     For example, if your Connector is running in Google Cloud, Cloud Manager uses the permissions from the Connector's service account to discover clusters running in Google Kubernetes Engine (GKE).

   ◦ Click **Import Cluster** to import a cluster using a kubeconfig file.

     After you upload the file, Cloud Manager verifies connectivity to the cluster and saves an encrypted copy of the kubeconfig file.

Result

Cloud Manager adds the Kubernetes cluster. You can now connect the cluster to Cloud Volumes ONTAP.

Connecting a cluster to Cloud Volumes ONTAP

Connect a Kubernetes cluster to Cloud Volumes ONTAP so you can use Cloud Volumes ONTAP as persistent storage for containers.

Steps

1. At the top of Cloud Manager, click **K8s**.

2. Click **Connect to Working Environment** for the cluster that you just added.
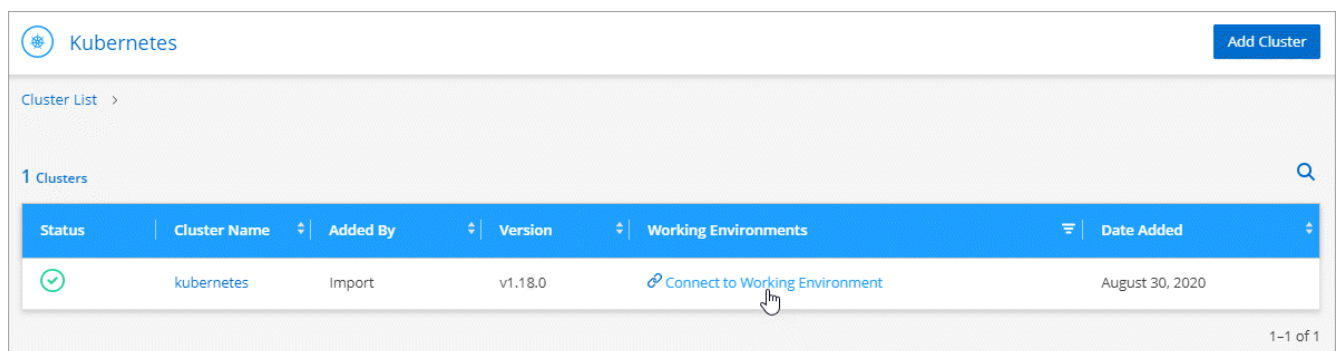
3. Select a working environment and click **Continue**.

4. Choose the NetApp storage class to use as the default storage class for the Kubernetes cluster and click **Continue**.

   When a user creates a persistent volume, the Kubernetes cluster can use this storage class as the backend storage by default.

5. Choose whether to use default auto export policies or whether to add a custom CIDR block.

6. Click **Add Working Environment**.

Result

Cloud Manager connects the working environment to the cluster, which can take up to 15 minutes.

Managing your clusters

Cloud Manager enables you to manage your Kubernetes clusters by changing the default storage class, upgrading Trident, and more.

Changing the default storage class

Make sure that you've set a Cloud Volumes ONTAP storage class as the default storage class so clusters use Cloud Volumes ONTAP as the backend storage.

Steps

1. At the top of Cloud Manager, click **K8s**.

2. Click the name of the Kubernetes cluster.

3. In the **Storage Classes** table, click the actions menu on the far right for the storage class that you'd like to set as the default.

4. Click **Set as Default**.

Upgrading Trident

You can upgrade Trident from Cloud Manager when a new version of Trident is available.

Steps

1. At the top of Cloud Manager, click **K8s**.

2. Click the name of the Kubernetes cluster.

3. If a new version is available, click **Upgrade** next to the Trident version.
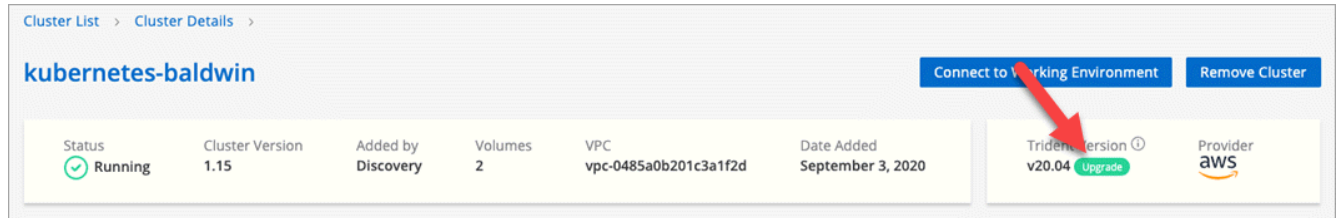
Updating the kubeconfig file

If you added your cluster to Cloud Manager by importing the kubeconfig file, you can upload the latest kubeconfig file to Cloud Manager at any time. You might do this if you've updated the credentials, if you've changed users or roles, or if something changed that affects the cluster, user, namespaces, or authentication.

Steps

1. At the top of Cloud Manager, click **K8s**.

2. Click the name of the Kubernetes cluster.

3. Click **Update Kubeconfig**.

4. When prompted through your web browser, select the updated kubeconfig file and click **Open**.

Result

Cloud Manager updates information about the Kubernetes cluster based on the latest kubeconfig file.

Disconnecting a cluster

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

Steps

1. At the top of Cloud Manager, click **K8s**.

2. Click the name of the Kubernetes cluster.

3. In the **Working Environments** table, click the actions menu on the far right for the working environment that you want to disconnect.

4. Click **Disconnect**.

Result

Cloud Manager disconnects the cluster from the Cloud Volumes ONTAP system.

Removing a cluster

Remove decommissioned clusters from Cloud Manager after you disconnect all working environments from the cluster.

Steps

1. At the top of Cloud Manager, click **K8s**.

2. Click the name of the Kubernetes cluster.

3. Click **Remove Cluster**.

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