Get started

Cloud Tiering

NetApp
May 04, 2022

This PDF was generated from https://docs.netapp.com/us-en/cloud-manager-tiering/concept-cloud-tiering.html on May 04, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Get started

Learn about Cloud Tiering

NetApp's Cloud Tiering service extends your data center to the cloud by automatically tiering inactive data from on-premises ONTAP clusters to object storage. This frees valuable space on the cluster for more workloads, without making changes to the application layer. Cloud Tiering can reduce costs in your data center and enables you to switch from a CAPEX model to an OPEX model.

The Cloud Tiering service leverages the capabilities of *FabricPool*. FabricPool is a NetApp Data Fabric technology that enables automated tiering of data to low-cost object storage. Active (hot) data remains on the local tier (on-premises ONTAP aggregates), while inactive (cold) data is moved to the cloud tier — all while preserving ONTAP data efficiencies.

Originally supported on AFF, FAS, and ONTAP Select systems with all-SSD aggregates, starting with ONTAP 9.8 you can tier data from aggregates consisting of HDDs in addition to high-performance SSDs. See the considerations and requirements for using FabricPool for details.

Cloud Tiering licenses can also be shared with your clusters that are in FabricPool Mirror configurations (not including MetroCluster configurations). The FabricPool configuration must be done using System Manager or the ONTAP CLI, but licensing for these types of clusters is done using Cloud Tiering.

Features

Cloud Tiering offers automation, monitoring, reports, and a common management interface:

- Automation makes it easier to set up and manage data tiering from on-prem ONTAP clusters to the cloud
- You can choose the default cloud provider storage class/access tier, or use lifecycle management to move older tiered data to a more cost-effective tier
- A single pane of glass removes the need to independently manage FabricPool across several clusters
- Reports show the amount of active and inactive data on each cluster
- A tiering health status helps you identify and correct issues as they occur
- If you have Cloud Volumes ONTAP systems, you'll find them in the Cluster Dashboard so you get a full view of data tiering in your hybrid cloud infrastructure

For more details about the value that Cloud Tiering provides, check out the Cloud Tiering page on NetApp Cloud Central.

Cloud Volumes ONTAP systems are read-only from Cloud Tiering. You set up tiering for Cloud Volumes ONTAP from the working environment in Cloud Manager.

Supported object storage providers

You can tier inactive data from an on-premises ONTAP system to the following object storage providers:

- Amazon S3
- Microsoft Azure Blob

- Google Cloud Storage
- S3-compatible object storage
- NetApp StorageGRID

Cloud Tiering licenses can also be shared with your clusters that are tiering data to IBM Cloud Object Storage. The FabricPool configuration must be done using System Manager or the ONTAP CLI, but licensing for this type of configuration is done using Cloud Tiering.

> You can tier data from NAS volumes to the public cloud or to private clouds, like StorageGRID. When tiering data that is accessed by SAN protocols, NetApp recommends using private clouds due to connectivity considerations.

Object storage tiers

Each ONTAP cluster tiers inactive data to a single object store. When you set up data tiering, you have the choice to add a new bucket/container or to select an existing bucket/container, along with a storage class or access tier.

- Learn about supported AWS S3 storage classes
- Learn about supported Azure Blob access tiers
- Learn about supported Google Cloud storage classes

Cloud Tiering uses the cloud provider default storage class/access tier for your inactive data. However, you can apply a lifecycle rule so that the data automatically transitions from the default storage class to another storage class after a certain number of days. This can help keep your costs down by moving very cold data to less expensive storage.

> You can't select lifecycle rules for data tiered to StorageGRID or S3-compatible storage.

Pricing and licenses

Pay for Cloud Tiering through a pay-as-you-go subscription, a bring-your-own Cloud Tiering license, or a combination of both. A 30-day free trial is available for your first cluster if you don't have a license.

There are no charges when tiering data to StorageGRID. Neither a BYOL license or PAYGO registration is required.

View pricing details.

30-day free trial

If you don't have a Cloud Tiering license, a 30-day free trial of Cloud Tiering starts when you set up tiering to your first cluster. After that 30-day free trial ends, you'll need to pay for Cloud Tiering through a pay-as-you-go subscription, a BYOL license, or a combination of both.

If your free trial ends and you haven't subscribed or added a license, then ONTAP no longer tiers cold data to object storage, but existing data is still available for access.

Pay-as-you-go subscription

Cloud Tiering offers consumption-based licensing in a pay-as-you-go model. After subscribing through your cloud provider's marketplace, you pay per GB for data that's tiered—there's no up-front payment. You are

billed by your cloud provider through your monthly bill.

You should subscribe even if you have a free trial or if you bring your own license (BYOL):

- Subscribing ensures that there's no disruption of service after your free trial ends.

  When the trial ends, you'll be charged hourly according to the amount of data that you tier.

- If you tier more data than allowed by your BYOL license, then data tiering continues through your pay-as-you-go subscription.

  For example, if you have a 10 TB license, all capacity beyond the 10 TB is charged through the pay-as-you-go subscription.

You won't be charged from your pay-as-you-go subscription during your free trial or if you haven't exceeded your Cloud Tiering BYOL license.

Learn how to set up a pay-as-you-go subscription.

Bring your own license

Bring your own license by purchasing a **Cloud Tiering** license from NetApp. You can purchase 2-, 12-, 24-, or 36-month term licenses and specify any amount of tiering capacity. The BYOL Cloud Tiering license is a *floating* license that you can use across multiple on-premises ONTAP clusters. The total tiering capacity that you define in your Cloud Tiering license can be used by all of your on-prem clusters.

After you purchase a Cloud Tiering license, you'll need use the Digital Wallet page in Cloud Manager to add the license. See how to use a Cloud Tiering BYOL license.

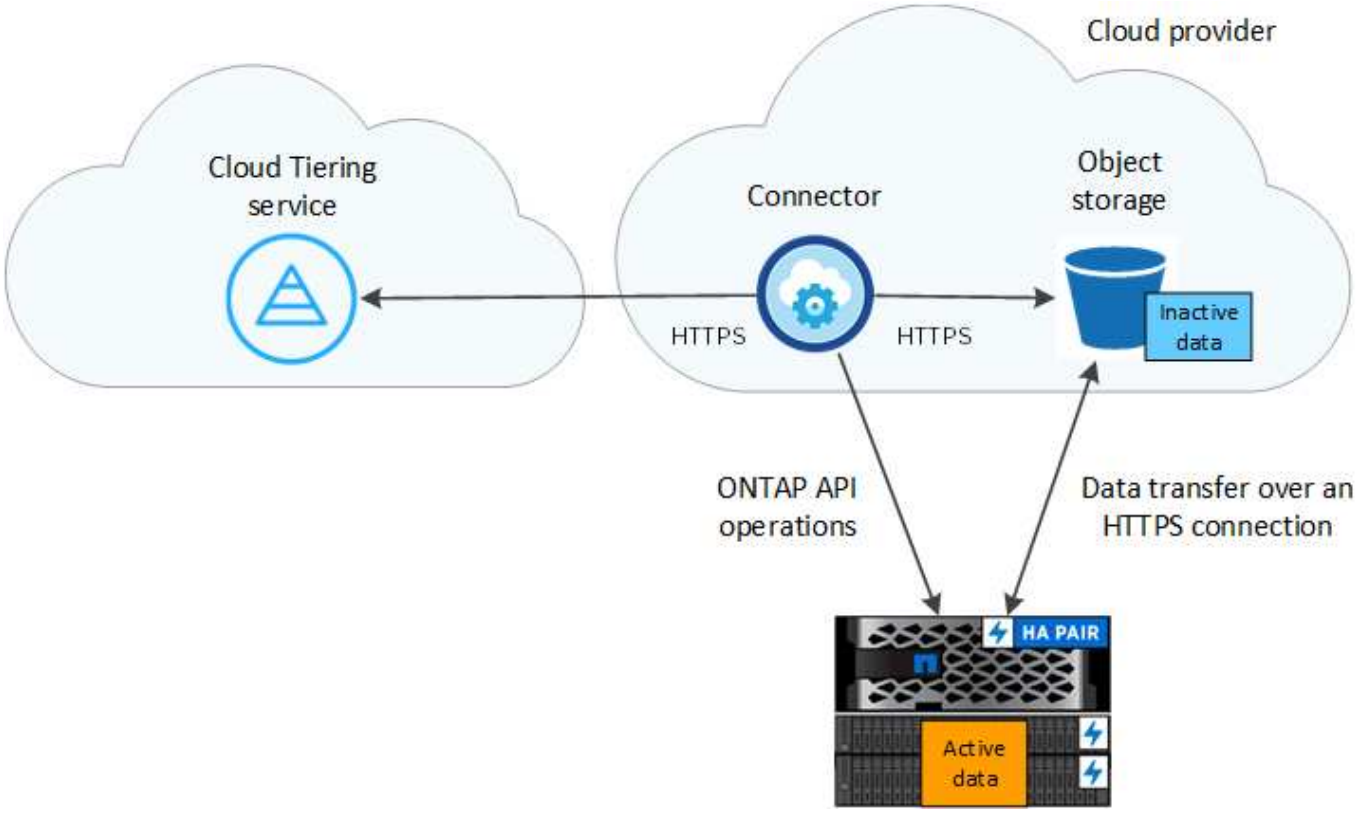
As noted above, we recommend that you set up a pay-as-you-go subscription, even if you have purchased a BYOL license.

Starting August 2021 the old **FabricPool** license was replaced by the **Cloud Tiering** license. Read more about how the Cloud Tiering license is different than the FabricPool license.

How Cloud Tiering works

Cloud Tiering is a NetApp-managed service that uses FabricPool technology to automatically tier inactive (cold) data from your on-premises ONTAP clusters to object storage in your public cloud or private cloud. Connections to ONTAP take place from a Connector.

The following image shows the relationship between each component:



At a high level, Cloud Tiering works like this:

1. You discover your on-prem cluster from Cloud Manager.
2. You set up tiering by providing details about your object storage, including the bucket/container, a storage class or access tier, and lifecycle rules for the tiered data.
3. Cloud Manager configures ONTAP to use the object storage provider and discovers the amount of active and inactive data on the cluster.
4. You choose the volumes to tier and the tiering policy to apply to those volumes.
5. ONTAP starts tiering inactive data to the object store as soon as the data has reached the thresholds to be considered inactive (see Volume tiering policies).
6. If you have applied a lifecycle rule to the tiered data (only available for some providers), older tiered data is moved to a more cost-effective tier after a certain number of days.

Volume tiering policies

When you select the volumes that you want to tier, you choose a *volume tiering policy* to apply to each volume. A tiering policy determines when or whether the user data blocks of a volume are moved to the cloud.

You can also adjust the **cooling period**. This is the number of days that user data in a volume must remain inactive before it is considered "cold" and moved to object storage. For tiering policies that allow you to adjust the cooling period, the valid values are 2 to 183 days when using ONTAP 9.8 and later, and 2 to 63 days for earlier ONTAP versions; 2 to 63 is the recommended best practice.

No Policy (None)

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

Cold snapshots (Snapshot only)

ONTAP tiers cold Snapshot blocks in the volume that are not shared with the active file system to object storage. If read, cold data blocks on the cloud tier become hot and are moved to the performance tier.

Data is tiered only after an aggregate has reached 50% capacity and when the data has reached the cooling period. The default number of cooling days is 2, but you can adjust this number.

> Re-heated data is written back to the performance tier only if there is space. If the performance tier capacity is more than 70% full, blocks continue to be accessed from the cloud tier.

Cold user data & snapshots (Auto)

ONTAP tiers all cold blocks in the volume (not including metadata) to object storage. The cold data includes not just Snapshot copies, but also cold user data from the active file system.

If read by random reads, cold data blocks on the cloud tier become hot and are moved to the performance tier. If read by sequential reads, such as those associated with index and antivirus scans, cold data blocks on the cloud tier stay cold and are not written to the performance tier. This policy is available starting with ONTAP 9.4.

Data is tiered only after an aggregate has reached 50% capacity and when the data has reached the cooling period. The default number of cooling days is 31, but you can adjust this number.

> Re-heated data is written back to the performance tier only if there is space. If the performance tier capacity is more than 70% full, blocks continue to be accessed from the cloud tier.

All user data (All)

All data (not including metadata) is immediately marked as cold and tiered to object storage as soon as possible. There is no need to wait 48 hours for new blocks in a volume to become cold. Note that blocks located in the volume prior to the All policy being set require 48 hours to become cold.

If read, cold data blocks on the cloud tier stay cold and are not written back to the performance tier. This policy is available starting with ONTAP 9.6.

Take the following into consideration before you choose this tiering policy:

- Tiering data immediately reduces storage efficiencies (inline only).
- You should use this policy only if you are confident that cold data on the volume will not change.
- Object storage is not transactional and will result in significant fragmentation if subjected to change.
- Consider the impact of SnapMirror transfers before assigning the All tiering policy to source volumes in data protection relationships.

  Because data is tiered immediately, SnapMirror will read data from the cloud tier rather than the performance tier. This will result in slower SnapMirror operations—possibly slowing other SnapMirror operations later in queue—even if they are using different tiering policies.

- Cloud Backup is similarly affected by volumes set with a tiering policy. See tiering policy considerations with Cloud Backup.

All DP user data (Backup)

All data on a data protection volume (not including metadata) is immediately moved to the cloud tier. If read, cold data blocks on the cloud tier stay cold and are not written back to the performance tier (starting with ONTAP 9.4).

This policy is available for ONTAP 9.5 or earlier. It was replaced with the **All** tiering policy starting with ONTAP 9.6.

Tier on-prem data to the cloud

Tiering data from on-premises ONTAP clusters to Amazon S3

Free space on your on-prem ONTAP clusters by tiering inactive data to Amazon S3.

Quick start

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

Prepare to tier data to Amazon S3

You need the following:

- An on-prem ONTAP cluster that's running ONTAP 9.2 or later and has an HTTPS connection to Amazon S3. Learn how to discover a cluster.
- An AWS account that has an access key and the required permissions so the ONTAP cluster can tier inactive data in and out of S3.
- A Connector installed in an AWS VPC or on your premises.
- Networking for the Connector that enables an outbound HTTPS connection to the ONTAP cluster, to S3 storage, and to the Cloud Tiering service.

Set up tiering

In Cloud Manager, select an on-prem working environment, click **Enable** for the Tiering service, and follow the prompts to tier data to Amazon S3.

Set up licensing

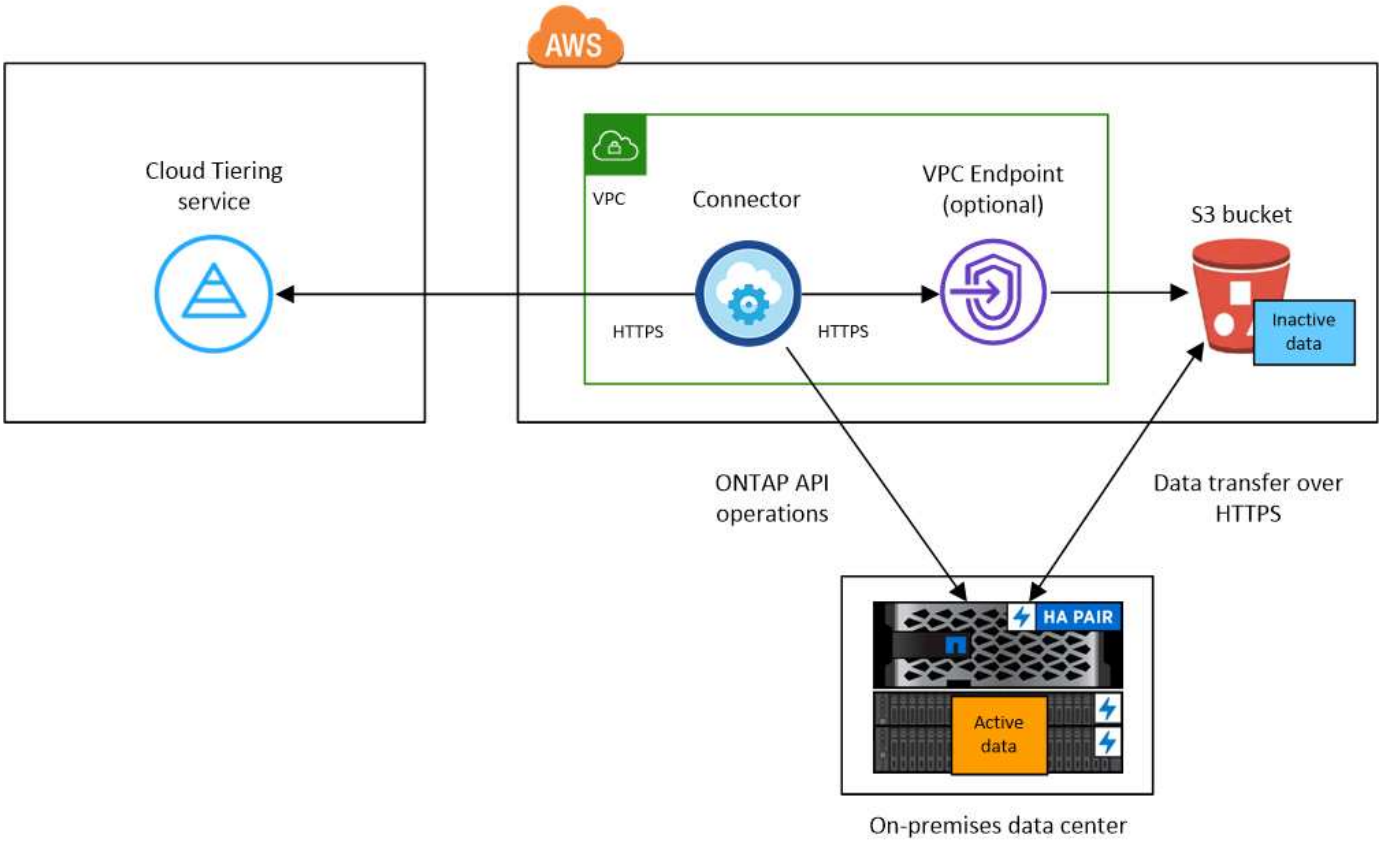
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP Cloud Tiering BYOL license, or a combination of both:

- To subscribe from the AWS Marketplace, go to the Cloud Manager Marketplace offering, click **Subscribe**, and then follow the prompts.
- To pay using a Cloud Tiering BYOL license, contact us if you need to purchase one, and then add it to your account from the Cloud Manager Digital Wallet.

Requirements

Verify support for your ONTAP cluster, set up your networking, and prepare your object storage.

The following image shows each component and the connections that you need to prepare between them:



Communication between a Connector and S3 is for object storage setup only. The Connector can reside on your premises, instead of in the cloud.

Preparing your ONTAP clusters

Your ONTAP clusters must meet the following requirements when tiering data to Amazon S3.

Supported ONTAP platforms

- When using ONTAP 9.8 and later: You can tier data from AFF systems, or FAS systems with all-SSD aggregates or all-HDD aggregates.
- When using ONTAP 9.7 and earlier: You can tier data from AFF systems, or FAS systems with all-SSD aggregates.

Supported ONTAP version

ONTAP 9.2 or later

Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over port 443 to Amazon S3.

  ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

Although AWS Direct Connect provides better performance and lower data transfer charges, it's not required between the ONTAP cluster and S3. But doing so is the recommended best practice.

- An inbound connection is required from the Connector, which can reside in an AWS VPC or on your premises.

  A connection between the cluster and the Cloud Tiering service is not required.

- An intercluster LIF is required on each ONTAP node that hosts the volumes you want to tier. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage.

  When you set up data tiering, Cloud Tiering prompts you for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created. Learn more about LIFs and IPspaces.

Supported volumes and aggregates

The total number of volumes that Cloud Tiering can tier might be less than the number of volumes on your ONTAP system. That's because volumes can't be tiered from some aggregates. Refer to ONTAP documentation for functionality or features not supported by FabricPool.

Cloud Tiering supports FlexGroup volumes starting with ONTAP 9.5. Setup works the same as any other volume.

Discovering an ONTAP cluster

You need to create an on-prem ONTAP working environment in Cloud Manager before you can start tiering cold data.

Learn how to discover a cluster.

Creating or switching Connectors

A Connector is required to tier data to the cloud. When tiering data to AWS S3, you can use a Connector that's in an AWS VPC or on your premises. You'll either need to create a new Connector or make sure that the currently selected Connector resides in AWS or on-prem.

- Learn about Connectors
- Creating a Connector in AWS
- Installing the Connector on a Linux host
- Switching between Connectors

Preparing networking for the Connector

Ensure that the Connector has the required networking connections. A Connector can be installed on-prem or in AWS.

Steps

1. Ensure that the network where the Connector is installed enables the following connections:
   - An outbound internet connection to the Cloud Tiering service over port 443 (HTTPS)
   - An HTTPS connection over port 443 to S3
   - An HTTPS connection over port 443 to your ONTAP cluster management LIF

2. If needed, enable a VPC Endpoint to S3.

   A VPC Endpoint to S3 is recommended if you have a Direct Connect or VPN connection from your ONTAP cluster to the VPC and you want communication between the Connector and S3 to stay in your AWS internal network.

Preparing Amazon S3

When you set up data tiering to a new cluster, you're prompted to create an S3 bucket or to select an existing S3 bucket in the AWS account where the Connector is set up. The AWS account must have permissions and an access key that you can enter in Cloud Tiering. The ONTAP cluster uses the access key to tier data in and out of S3.

The S3 bucket must be in a region that supports Cloud Tiering.

> If you are planning to configure Cloud Tiering to use a lower cost storage class where your tiered data will transition to after a certain number of days, you must not select any life cycle rules when setting up the bucket in your AWS account. Cloud Tiering manages the life cycle transitions.

Steps

1. Provide the following permissions to the IAM user:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject"
```

   AWS Documentation: Creating a Role to Delegate Permissions to an IAM User

2. Create or locate an access key.

   Cloud Tiering passes the access key on to the ONTAP cluster. The credentials are not stored in the Cloud Tiering service.

   AWS Documentation: Managing Access Keys for IAM Users

Tiering inactive data from your first cluster to Amazon S3

After you prepare your AWS environment, start tiering inactive data from your first cluster.

What you'll need

- An on-premises working environment.
- An AWS access key for an IAM user who has the required S3 permissions.

Steps

1. Select an on-prem cluster.

2. Click **Enable** for the Tiering service.

3. **Choose your provider**: This page appears only when using an on-prem Connector. Select **Amazon Web Services** and click **Continue**.
4. Complete the steps on the **Tiering Setup** page:
   a. **S3 Bucket**: Add a new S3 bucket or select an existing S3 bucket that starts with the prefix *fabric-pool* and click **Continue**.

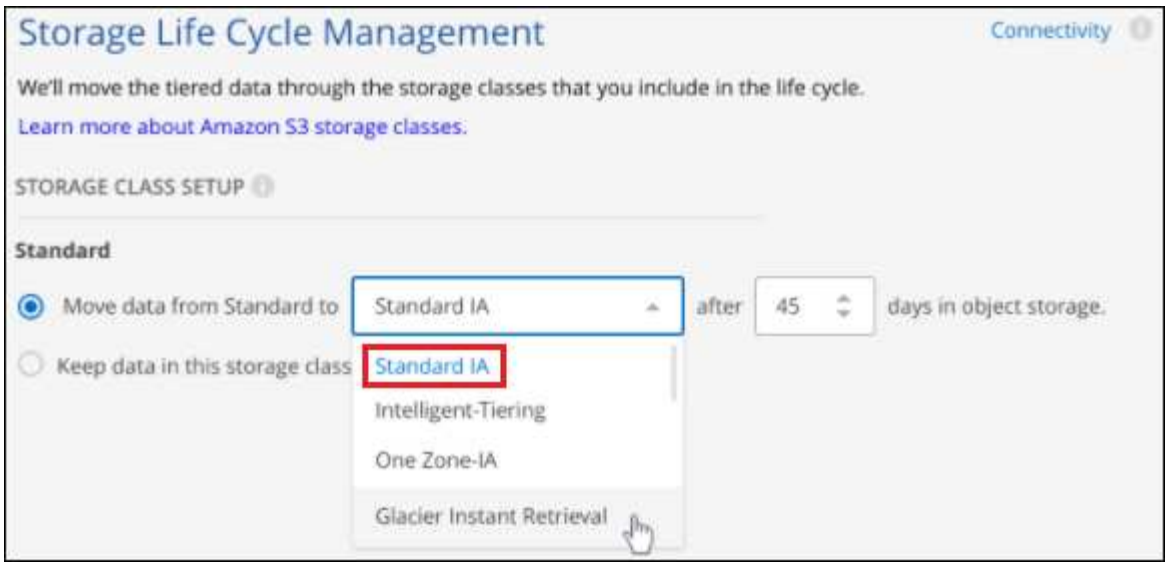
      When using an on-prem Connector, you must enter the AWS Account ID that provides access to the existing S3 bucket or new S3 bucket that will be created.

      The *fabric-pool* prefix is required because the IAM policy for the Connector enables the instance to perform S3 actions on buckets named with that exact prefix. For example, you could name the S3 bucket *fabric-pool-AFF1*, where AFF1 is the name of the cluster.

   b. **Storage Class Life Cycle**: Cloud Tiering manages the life cycle transitions of your tiered data. Data starts in the *Standard* class, but you can create a rule to move the data to another class after a certain number of days.

      Select the S3 storage class that you want to transition the tiered data to and the number of days before the data will be moved, and click **Continue**. For example, the screenshot below shows that tiered data is moved from the *Standard* class to the *Standard-IA* class after 45 days in object storage.

      If you choose **Keep data in this storage class**, then the data remains in the *Standard* storage class and no rules are applied. See supported storage classes.



Note that the life cycle rule is applied to all objects in the selected bucket.

c. **Credentials**: Enter the access key ID and secret key for an IAM user who has the required S3 permissions, and click **Continue**.

The IAM user must be in the same AWS account as the bucket that you selected or created on the **S3 Bucket** page.

d. **Cluster Network**: Select the IPspace that ONTAP should use to connect to object storage, and click **Continue**.

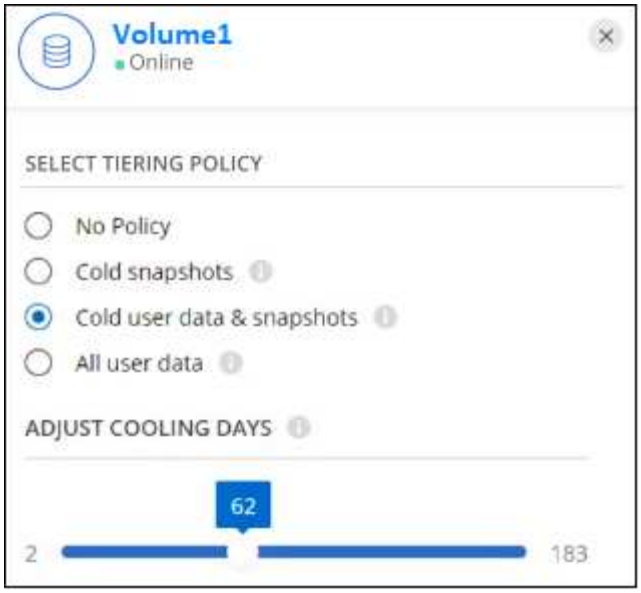
Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your cloud provider's object storage.

5. On the *Tier Volumes* page, select the volumes that you want to configure tiering for and launch the Tiering Policy page:

   - To select all volumes, check the box in the title row (Volume Name) and click **Configure volumes**.
   - To select multiple volumes, check the box for each volume (Volume_1) and click **Configure volumes**.
   - To select a single volume, click the row (or icon) for the volume.

6. In the *Tiering Policy* dialog, select a tiering policy, optionally adjust the cooling days for the selected volumes, and click **Apply**.

   Learn more about volume tiering policies and cooling days.



Result

You've successfully set up data tiering from volumes on the cluster to S3 object storage.

What's next?

Be sure to subscribe to the Cloud Tiering service.

You can also add additional clusters or review information about the active and inactive data on the cluster. For details, see Managing data tiering from your clusters.

Tiering data from on-premises ONTAP clusters to Azure Blob storage

Free space on your on-prem ONTAP clusters by tiering inactive data to Azure Blob storage.

Quick start

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

1 Prepare to tier data to Azure Blob storage

You need the following:

- An on-prem ONTAP cluster that's running ONTAP 9.4 or later and has an HTTPS connection to Azure Blob storage. Learn how to discover a cluster.
- A Connector installed in an Azure VNet or on your premises.
- Networking for a Connector that enables an outbound HTTPS connection to the ONTAP cluster in your data center, to Azure storage, and to the Cloud Tiering service.

2 Set up tiering

In Cloud Manager, select an on-prem working environment, click **Enable** for the Tiering service, and follow the prompts to tier data to Azure Blob storage.

3 Set up licensing

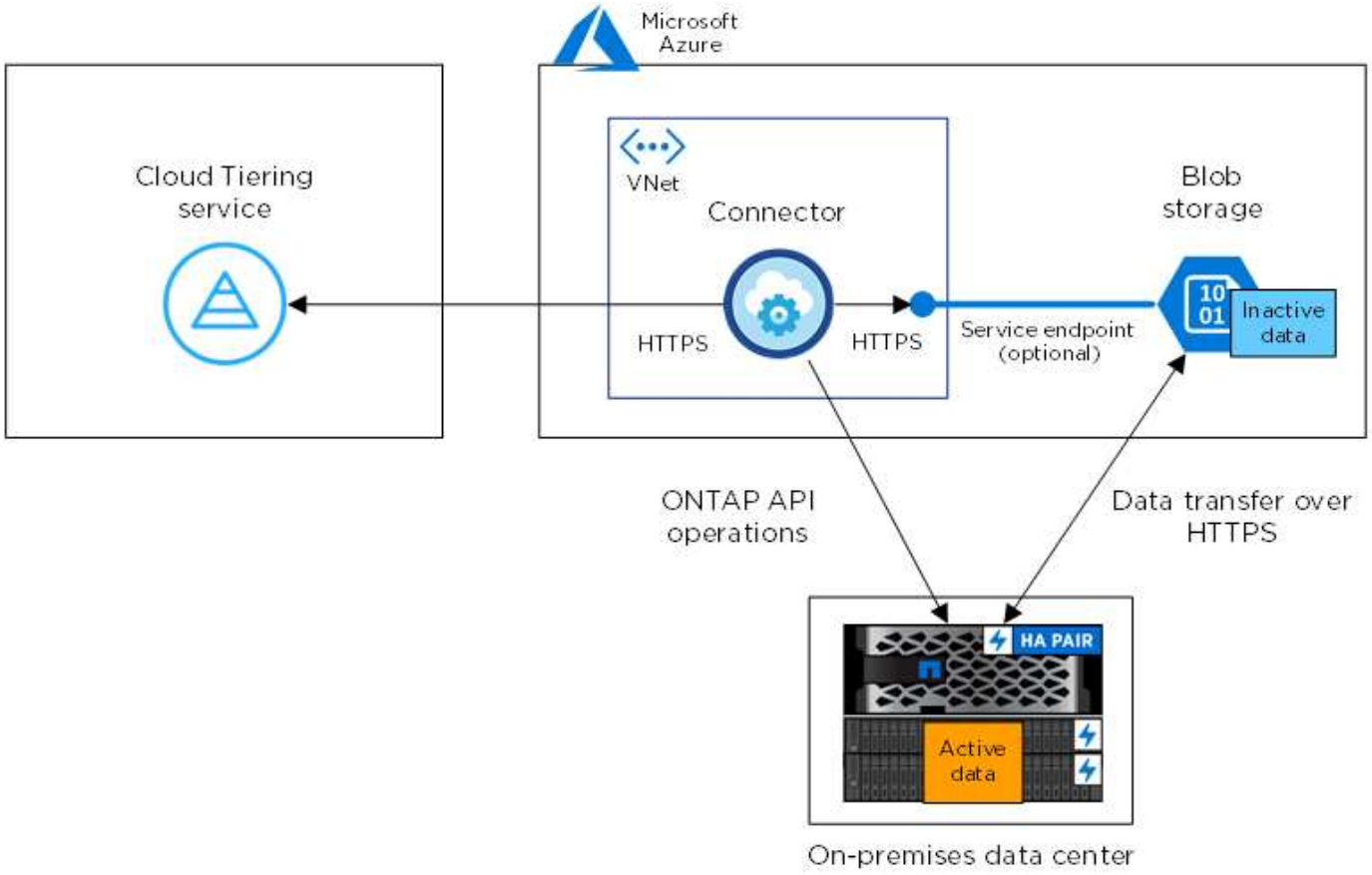
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP Cloud Tiering BYOL license, or a combination of both:

- To subscribe from the Azure Marketplace, go to the Cloud Manager Marketplace offering, click **Subscribe**, and then follow the prompts.
- To pay using a Cloud Tiering BYOL license, contact us if you need to purchase one, and then add it to your account from the Cloud Manager Digital Wallet.

Requirements

Verify support for your ONTAP cluster, set up your networking, and prepare your object storage.

The following image shows each component and the connections that you need to prepare between them:



Communication between the Connector and Blob storage is for object storage setup only. The Connector can reside on your premises, instead of in the cloud.

Preparing your ONTAP clusters

Your ONTAP clusters must meet the following requirements when tiering data to Azure Blob storage.

Supported ONTAP platforms

- When using ONTAP 9.8 and later: You can tier data from AFF systems, or FAS systems with all-SSD aggregates or all-HDD aggregates.

- When using ONTAP 9.7 and earlier: You can tier data from AFF systems, or FAS systems with all-SSD aggregates.

Supported ONTAP version

ONTAP 9.4 or later

Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over port 443 to Azure Blob storage.

  ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

  Although ExpressRoute provides better performance and lower data transfer charges, it's not required between the ONTAP cluster and Azure Blob storage. But doing so is the recommended best practice.

- An inbound connection is required from the Connector, which can reside in an Azure VNet or on your premises.

  A connection between the cluster and the Cloud Tiering service is not required.

- An intercluster LIF is required on each ONTAP node that hosts the volumes you want to tier. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage.

  When you set up data tiering, Cloud Tiering prompts you for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created. Learn more about LIFs and IPspaces.

Supported volumes and aggregates

The total number of volumes that Cloud Tiering can tier might be less than the number of volumes on your ONTAP system. That's because volumes can't be tiered from some aggregates. Refer to ONTAP documentation for functionality or features not supported by FabricPool.

Cloud Tiering supports FlexGroup volumes, starting with ONTAP 9.5. Setup works the same as any other volume.

Discovering an ONTAP cluster

You need to create an on-prem ONTAP working environment in Cloud Manager before you can start tiering cold data.

Learn how to discover a cluster.

Creating or switching Connectors

A Connector is required to tier data to the cloud. When tiering data to Azure Blob storage, you can use a Connector that's in an Azure VNet or on your premises. You'll either need to create a new Connector or make sure that the currently selected Connector resides in Azure or on-prem.

- Learn about Connectors
- Creating a Connector in Azure
- Installing the Connector on a Linux host
- Switching between Connectors

Verify that you have the necessary Connector permissions

If you created the Connector using Cloud Manager version 3.9.7 or greater, then you're all set.

If you created the Connector using an earlier version of Cloud Manager, then you'll need to edit the permission list to add 2 required permissions:

```
Microsoft.Storage/storageAccounts/managementPolicies/read
Microsoft.Storage/storageAccounts/managementPolicies/write
```

Preparing networking for the Connector

Ensure that the Connector has the required networking connections. A Connector can be installed on-prem or in Azure.

Steps

1. Ensure that the network where the Connector is installed enables the following connections:
   - An outbound internet connection to the Cloud Tiering service over port 443 (HTTPS)
   - An HTTPS connection over port 443 to Azure Blob storage
   - An HTTPS connection over port 443 to your ONTAP cluster management LIF
2. If needed, enable a VNet service endpoint to Azure storage.

   A VNet service endpoint to Azure storage is recommended if you have an ExpressRoute or VPN connection from your ONTAP cluster to the VNet and you want communication between the Connector and Blob storage to stay in your virtual private network.

Preparing Azure Blob storage

When you set up tiering, you need to identify the resource group you want to use, and the storage account and Azure container that belong to the resource group. A storage account enables Cloud Tiering to authenticate and access the Blob container used for data tiering.

Cloud Tiering supports only the General Purpose v2 and Premium Block Blob types of storage accounts.

The Blob container must be in a region that supports Cloud Tiering.

> If you are planning to configure Cloud Tiering to use a lower cost access tier where your tiered data will transition to after a certain number of days, you must not select any life cycle rules when setting up the container in your Azure account. Cloud Tiering manages the life cycle transitions.

Tiering inactive data from your first cluster to Azure Blob storage

After you prepare your Azure environment, start tiering inactive data from your first cluster.

What you'll need

An on-premises working environment.

Steps

1. Select an on-prem cluster.

2. Click **Enable** for the Tiering service.

3. **Choose your provider**: This page appears only when using an on-prem Connector. Select **Microsoft Azure** and click **Continue**.
4. Complete the steps on the **Tiering Setup** page:
   a. **Resource Group**: Select a resource group where an existing container is managed, or where you would like to create a new container for tiered data, and click **Continue**.
   b. **Azure Container**: Add a new Blob container to a storage account, or select an existing container, and click **Continue**.

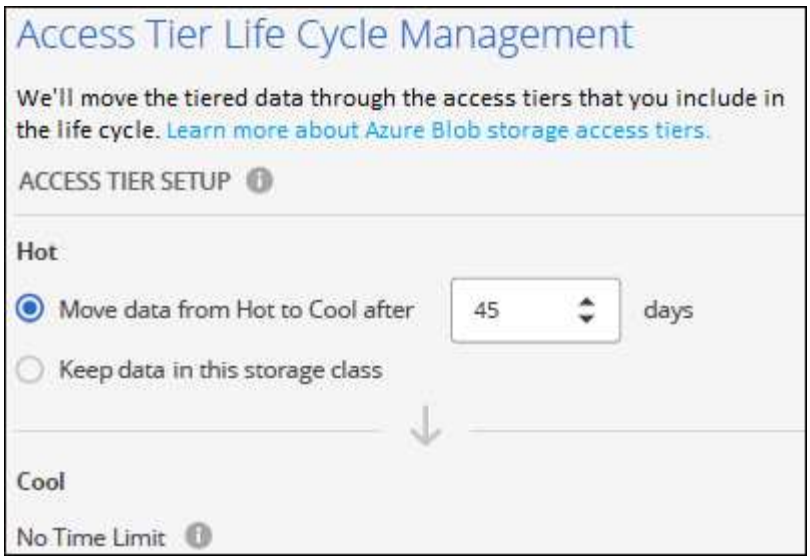
      When using an on-prem Connector, you must enter the Azure Subscription that provides access to the existing container or new container that will be created.

      The storage account and containers that appear in this step belong to the resource group that you selected in the previous step.

   c. **Access Tier Life Cycle**: Cloud Tiering manages the life cycle transitions of your tiered data. Data starts in the *Hot* class, but you can create a rule to move the data to the *Cool* class after a certain number of days.

      Select the access tier that you want to transition the tiered data to and the number of days before the data will be moved, and click **Continue**. For example, the screenshot below shows that tiered data is moved from the *Hot* class to the *Cool* class after 45 days in object storage.

      If you choose **Keep data in this access tier**, then the data remains in the *Hot* access tier and no rules are applied. See supported access tiers.



Note that the life cycle rule is applied to all blob containers in the selected storage account.

Verify that you have the necessary Connector permissions for the life cycle management feature.

d. **Cluster Network**: Select the IPspace that ONTAP should use to connect to object storage, and click **Continue**.

Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your cloud provider's object storage.

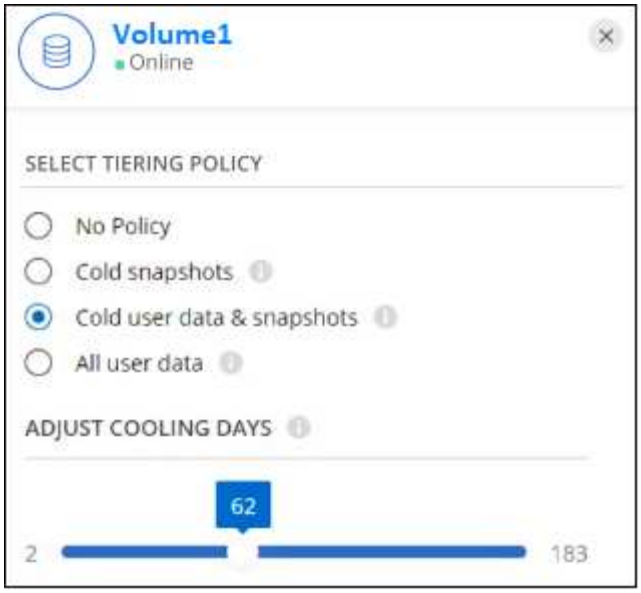
5. On the *Tier Volumes* page, select the volumes that you want to configure tiering for and launch the Tiering Policy page:
   - To select all volumes, check the box in the title row (

) and click **Configure volumes**.
   - To select multiple volumes, check the box for each volume (

) and click **Configure volumes**.
   - To select a single volume, click the row (or  icon) for the volume.

6. In the *Tiering Policy* dialog, select a tiering policy, optionally adjust the cooling days for the selected volumes, and click **Apply**.

Learn more about volume tiering policies and cooling days.



Result

You've successfully set up data tiering from volumes on the cluster to Azure Blob object storage.

What's next?

Be sure to subscribe to the Cloud Tiering service.

You can also add additional clusters or review information about the active and inactive data on the cluster. For details, see Managing data tiering from your clusters.

Tiering data from on-premises ONTAP clusters to Google Cloud Storage

Free space on your on-prem ONTAP clusters by tiering inactive data to Google Cloud Storage.

Quick start

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

1 Prepare to tier data to Google Cloud Storage

You need the following:

- An on-prem ONTAP cluster that's running ONTAP 9.6 or later and has an HTTPS connection to Google Cloud Storage. Learn how to discover a cluster.
- A service account that has the predefined Storage Admin role and storage access keys.
- A Connector installed in a Google Cloud Platform VPC.
- Networking for the Connector that enables an outbound HTTPS connection to the ONTAP cluster in your data center, to Google Cloud Storage, and to the Cloud Tiering service.

2 Set up tiering

In Cloud Manager, select an on-prem working environment, click **Enable** for the Tiering service, and follow the

prompts to tier data to Google Cloud Storage.

3 Set up licensing

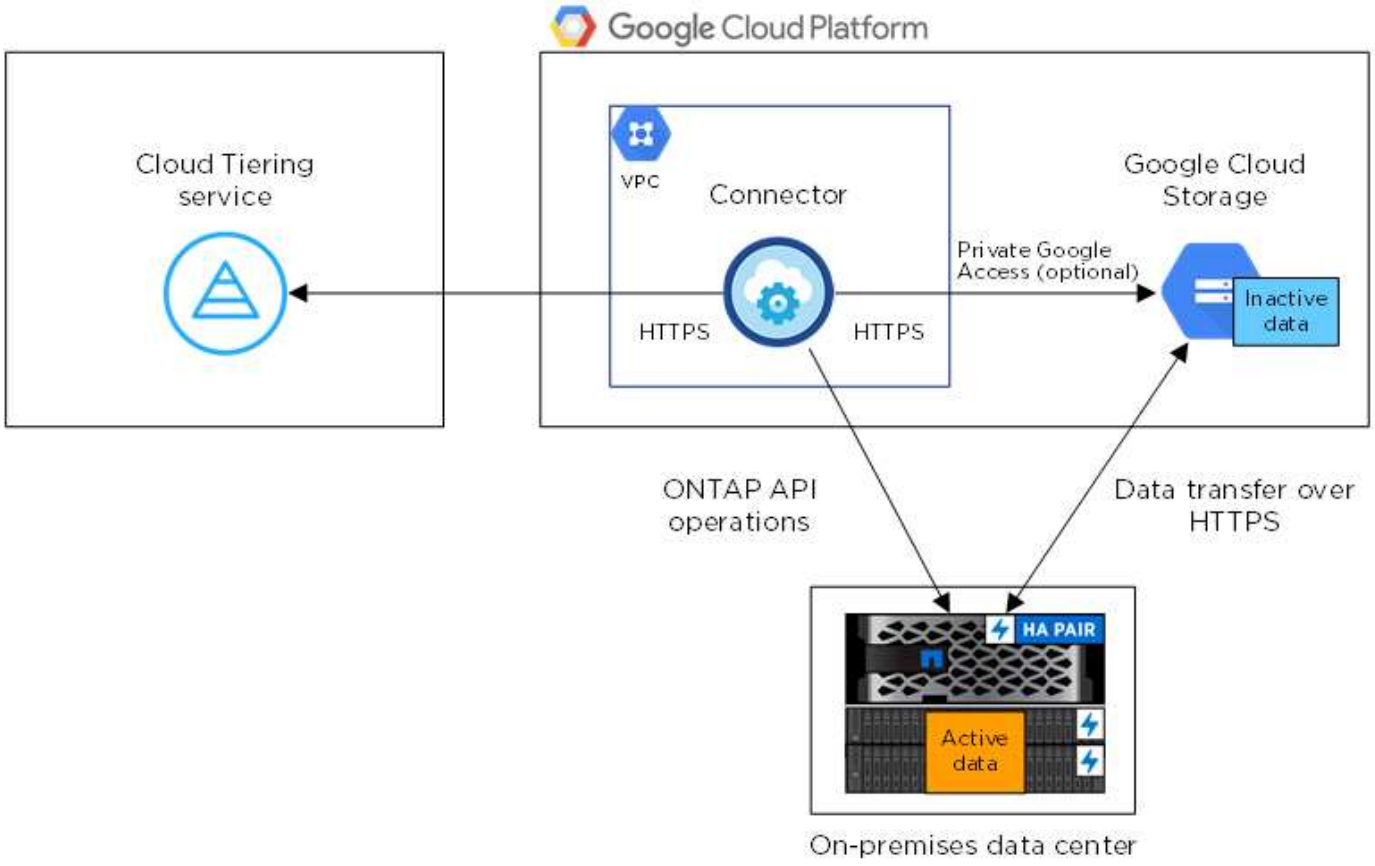
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP Cloud Tiering BYOL license, or a combination of both:

- To subscribe from the GCP Marketplace, go to the Cloud Manager Marketplace offering, click **Subscribe**, and then follow the prompts.
- To pay using a Cloud Tiering BYOL license, contact us if you need to purchase one, and then add it to your account from the Cloud Manager Digital Wallet.

Requirements

Verify support for your ONTAP cluster, set up your networking, and prepare your object storage.

The following image shows each component and the connections that you need to prepare between them:



Communication between the Connector and Google Cloud Storage is for object storage setup only.

Preparing your ONTAP clusters

Your ONTAP clusters must meet the following requirements when tiering data to Google Cloud Storage.

Supported ONTAP platforms

- When using ONTAP 9.8 and later: You can tier data from AFF systems, or FAS systems with all-SSD aggregates or all-HDD aggregates.
- When using ONTAP 9.7 and earlier: You can tier data from AFF systems, or FAS systems with all-SSD aggregates.

Supported ONTAP versions

ONTAP 9.6 or later

Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over port 443 to Google Cloud Storage.

  ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

  Although a Google Cloud Interconnect provides better performance and lower data transfer charges, it's not required between the ONTAP cluster and Google Cloud Storage. But doing so is the recommended best practice.

- An inbound connection is required from the Connector, which resides in a Google Cloud Platform VPC.

  A connection between the cluster and the Cloud Tiering service is not required.

- An intercluster LIF is required on each ONTAP node that hosts the volumes you want to tier. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage.

  When you set up data tiering, Cloud Tiering prompts you for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created. Learn more about LIFs and IPspaces.

Supported volumes and aggregates

The total number of volumes that Cloud Tiering can tier might be less than the number of volumes on your ONTAP system. That's because volumes can't be tiered from some aggregates. Refer to ONTAP documentation for functionality or features not supported by FabricPool.

Cloud Tiering supports FlexGroup volumes. Setup works the same as any other volume.

Discovering an ONTAP cluster

You need to create an on-prem ONTAP working environment in Cloud Manager before you can start tiering cold data.

Learn how to discover a cluster.

Creating or switching Connectors

A Connector is required to tier data to the cloud. When tiering data to Google Cloud Storage, a Connector must be available in a Google Cloud Platform VPC. You'll either need to create a new Connector or make sure that the currently selected Connector resides in GCP.

- Learn about Connectors
- Creating a Connector in GCP

- Switching between Connectors

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

1. Ensure that the VPC where the Connector is installed enables the following connections:
   - An outbound internet connection to the Cloud Tiering service over port 443 (HTTPS)
   - An HTTPS connection over port 443 to Google Cloud Storage
   - An HTTPS connection over port 443 to your ONTAP cluster management LIF
2. Optional: Enable Private Google Access on the subnet where you plan to deploy the Connector.

   Private Google Access is recommended if you have a direct connection from your ONTAP cluster to the VPC and you want communication between the Connector and Google Cloud Storage to stay in your virtual private network. Note that Private Google Access works with VM instances that have only internal (private) IP addresses (no external IP addresses).

Preparing Google Cloud Storage

When you set up tiering, you need to provide storage access keys for a service account that has Storage Admin permissions. A service account enables Cloud Tiering to authenticate and access Cloud Storage buckets used for data tiering. The keys are required so that Google Cloud Storage knows who is making the request.

The Cloud Storage buckets must be in a region that supports Cloud Tiering.

> If you are planning to configure Cloud Tiering to use lower cost storage classes where your tiered data will transition to after a certain number of days, you must not select any life cycle rules when setting up the bucket in your GCP account. Cloud Tiering manages the life cycle transitions.

Steps

1. Create a service account that has the predefined Storage Admin role.
2. Go to GCP Storage Settings and create access keys for the service account:
   a. Select a project, and click **Interoperability**. If you haven't already done so, click **Enable interoperability access**.
   b. Under **Access keys for service accounts**, click **Create a key for a service account**, select the service account that you just created, and click **Create Key**.

      You'll need to enter the keys later when you set up Cloud Tiering.

Tiering inactive data from your first cluster to Google Cloud Storage

After you prepare your Google Cloud environment, start tiering inactive data from your first cluster.

What you'll need

- An on-premises working environment.
- Storage access keys for a service account that has the Storage Admin role.

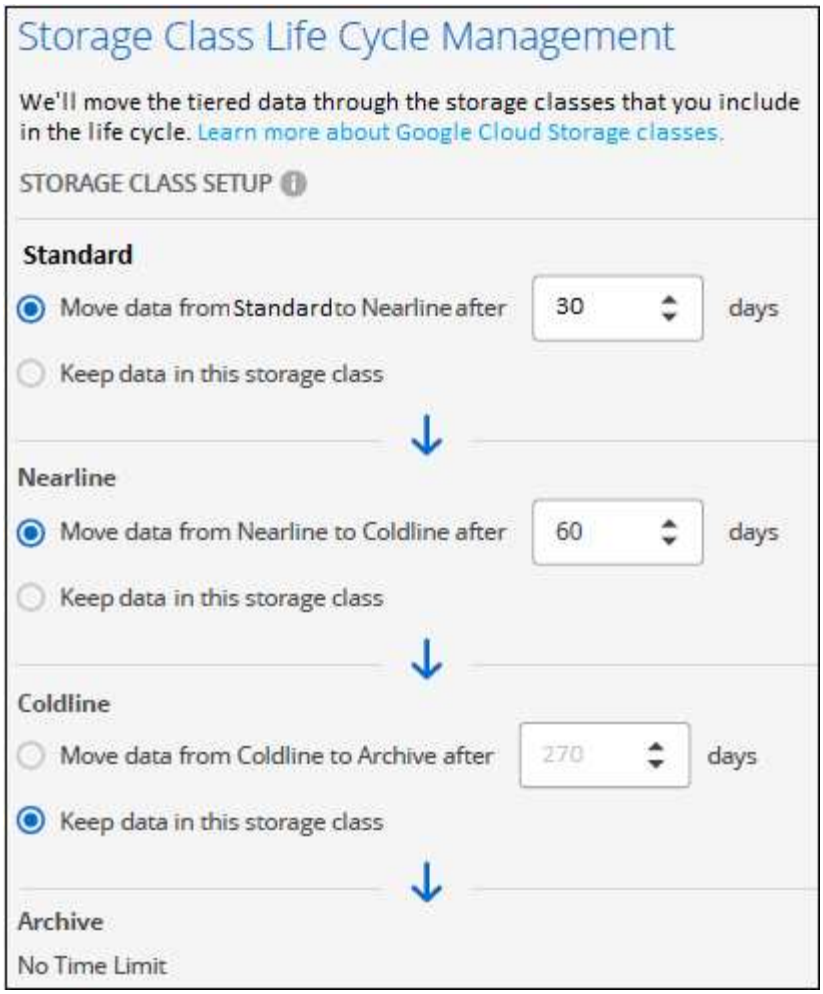
Steps

1. Select an on-prem cluster.
2. Click **Enable** for the Tiering service.

3. Complete the steps on the **Tiering Setup** page:
   a. **Bucket**: Add a new Google Cloud Storage bucket or select an existing bucket.
   b. **Storage Class Life Cycle**: Cloud Tiering manages the life cycle transitions of your tiered data. Data starts in the *Standard* class, but you can create rules to move the data to other classes after a certain number of days.

      Select the Google Cloud storage class that you want to transition the tiered data to and the number of days before the data will be moved, and click **Continue**. For example, the screenshot below shows that tiered data is moved from the *Standard* class to the *Nearline* class after 30 days in object storage, and then to the *Coldline* class after 60 days in object storage.

      If you choose **Keep data in this storage class**, then the data remains in the that storage class. See supported storage classes.



Note that the life cycle rule is applied to all objects in the selected bucket.

c. **Credentials**: Enter the storage access key and secret key for a service account that has the Storage Admin role.

d. **Cluster Network**: Select the IPspace that ONTAP should use to connect to object storage.

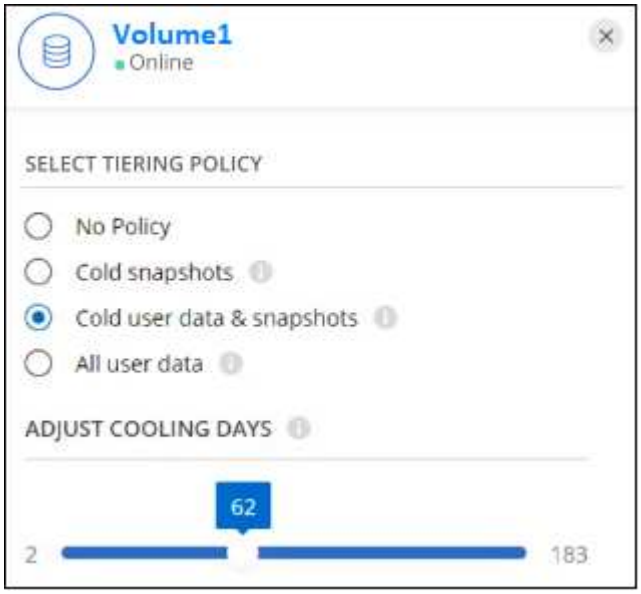
Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your cloud provider's object storage.

4. Click **Continue** to select the volumes that you want to tier.
5. On the *Tier Volumes* page, select the volumes that you want to configure tiering for and launch the Tiering Policy page:
   - To select all volumes, check the box in the title row (

) and click **Configure volumes**.
   - To select multiple volumes, check the box for each volume (

) and click **Configure volumes**.
   - To select a single volume, click the row (or  icon) for the volume.
6. In the *Tiering Policy* dialog, select a tiering policy, optionally adjust the cooling days for the selected volumes, and click **Apply**.

Learn more about volume tiering policies and cooling days.



Result

You've successfully set up data tiering from volumes on the cluster to Google Cloud object storage.

What's next?

Be sure to subscribe to the Cloud Tiering service.

You can also add additional clusters or review information about the active and inactive data on the cluster. For details, see Managing data tiering from your clusters.

Tiering data from on-premises ONTAP clusters to StorageGRID

Free space on your on-prem ONTAP clusters by tiering inactive data to StorageGRID.

Quick start

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

1 Prepare to tier data to StorageGRID

You need the following:

- An on-prem ONTAP cluster that's running ONTAP 9.4 or later, and a connection over a user-specified port to StorageGRID. Learn how to discover a cluster.
- StorageGRID 10.3 or later with AWS access keys that have S3 permissions.
- A Connector installed on your premises.
- Networking for the Connector that enables an outbound HTTPS connection to the ONTAP cluster, to StorageGRID, and to the Cloud Tiering service.

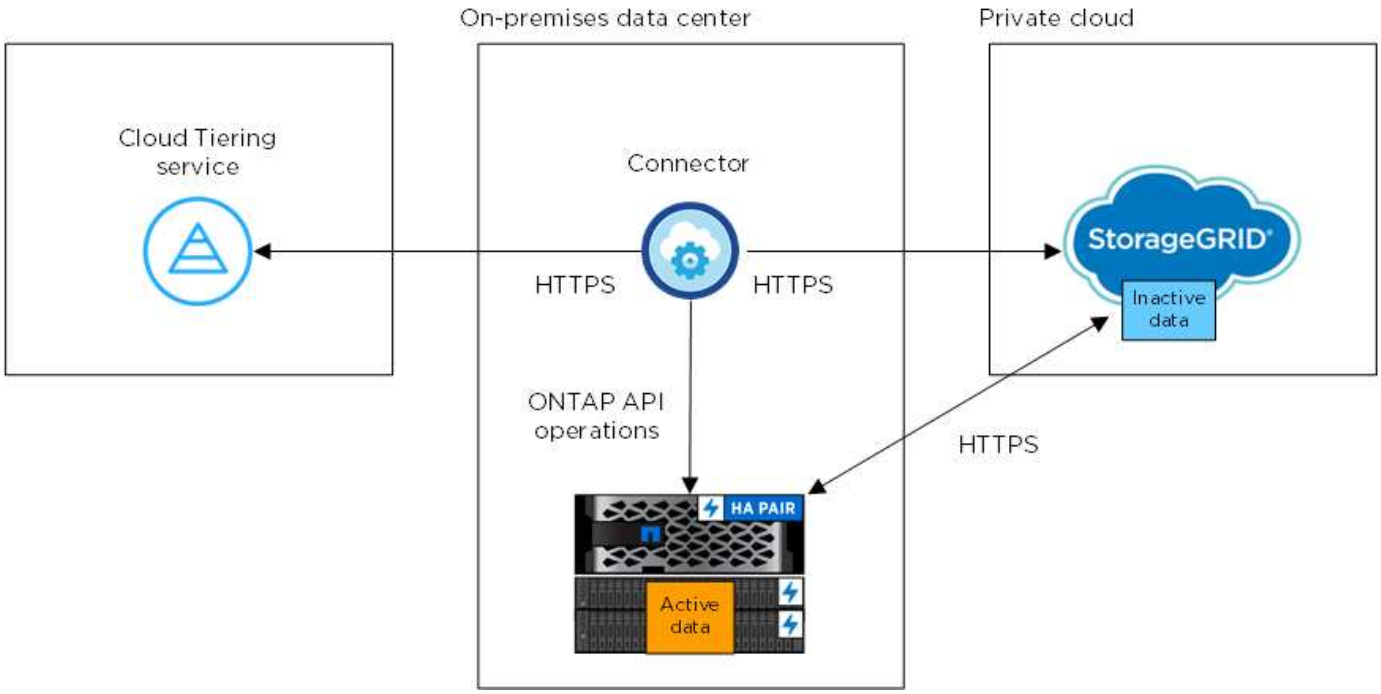
2 Set up tiering

In Cloud Manager, select an on-prem working environment, click **Enable** for the Tiering service, and follow the prompts to tier data to StorageGRID.

Requirements

Verify support for your ONTAP cluster, set up your networking, and prepare your object storage.

The following image shows each component and the connections that you need to prepare between them:



Communication between the Connector and StorageGRID is for object storage setup only.

Preparing your ONTAP clusters

Your ONTAP clusters must meet the following requirements when tiering data to StorageGRID.

Supported ONTAP platforms

- When using ONTAP 9.8 and later: You can tier data from AFF systems, or FAS systems with all-SSD aggregates or all-HDD aggregates.
- When using ONTAP 9.7 and earlier: You can tier data from AFF systems, or FAS systems with all-SSD aggregates.

Supported ONTAP version

ONTAP 9.4 or later

Licensing

A Cloud Tiering license isn't required in your Cloud Manager account, nor is a FabricPool license required on the ONTAP cluster, when tiering data to StorageGRID.

Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over a user-specified port to StorageGRID (the port is configurable during tiering setup).

ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

- An inbound connection is required from the Connector, which must reside on your premises.

  A connection between the cluster and the Cloud Tiering service is not required.

- An intercluster LIF is required on each ONTAP node that hosts the volumes you want to tier. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage.

  When you set up data tiering, Cloud Tiering prompts you for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created. Learn more about LIFs and IPspaces.

Supported volumes and aggregates

The total number of volumes that Cloud Tiering can tier might be less than the number of volumes on your ONTAP system. That's because volumes can't be tiered from some aggregates. Refer to ONTAP documentation for functionality or features not supported by FabricPool.

Cloud Tiering supports FlexGroup volumes, starting with ONTAP 9.5. Setup works the same as any other volume.

Discovering an ONTAP cluster

You need to create an on-prem ONTAP working environment in the Cloud Manager Canvas before you can start tiering cold data.

Learn how to discover a cluster.

Preparing StorageGRID

StorageGRID must meet the following requirements.

Supported StorageGRID versions

StorageGRID 10.3 and later is supported.

S3 credentials

When you set up tiering to StorageGRID, you need to provide Cloud Tiering with an S3 access key and secret key. Cloud Tiering uses the keys to access your buckets.

These access keys must be associated with a user who has the following permissions:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Object versioning

You must not enable StorageGRID object versioning on the object store bucket.

Creating or switching Connectors

A Connector is required to tier data to the cloud. When tiering data to StorageGRID, a Connector must be available on your premises. You'll either need to install a new Connector or make sure that the currently selected Connector resides on-prem.

- Learn about Connectors
- Installing the Connector on a Linux host
- Switching between Connectors

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

1. Ensure that the network where the Connector is installed enables the following connections:
    - An outbound internet connection to the Cloud Tiering service over port 443 (HTTPS)
    - An HTTPS connection over port 443 to StorageGRID
    - An HTTPS connection over port 443 to your ONTAP cluster management LIF

Tiering inactive data from your first cluster to StorageGRID

After you prepare your environment, start tiering inactive data from your first cluster.

What you'll need

- An on-premises working environment.
- The FQDN of the StorageGRID server and the port that will be used for HTTPS communications.
- An AWS access key that has the required S3 permissions.

Steps

1. Select an on-prem cluster.
2. Click **Enable** for the Tiering service.

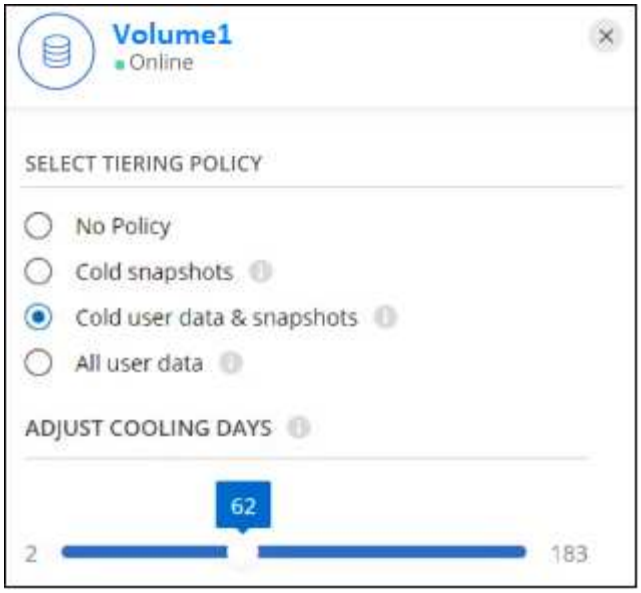
3. **Choose your provider**: Select **StorageGRID** and click **Continue**.
4. Complete the steps on the **Tiering Setup** page:
   a. **Server**: Enter the FQDN of the StorageGRID server, the port that ONTAP should use for HTTPS communication with StorageGRID, and the access key and secret key for an account that has the required S3 permissions.
   b. **Bucket**: Add a new bucket or select an existing bucket that starts with the prefix *fabric-pool* and click **Continue**.

      The *fabric-pool* prefix is required because the IAM policy for the Connector enables the instance to perform S3 actions on buckets named with that exact prefix. For example, you could name the S3 bucket *fabric-pool-AFF1*, where AFF1 is the name of the cluster.

   c. **Cluster Network**: Select the IPspace that ONTAP should use to connect to object storage and click **Continue**.

      Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to StorageGRID object storage.
5. On the *Tier Volumes* page, select the volumes that you want to configure tiering for and launch the Tiering Policy page:
   - To select all volumes, check the box in the title row (Volume Name) and click **Configure volumes**.
   - To select multiple volumes, check the box for each volume (Volume_1) and click **Configure volumes**.
   - To select a single volume, click the row (or icon) for the volume.
6. In the *Tiering Policy* dialog, select a tiering policy, optionally adjust the cooling days for the selected volumes, and click **Apply**.

   Learn more about volume tiering policies and cooling days.



Result

You've successfully set up data tiering from volumes on the cluster to StorageGRID.

What's next?

You can add additional clusters or review information about the active and inactive data on the cluster. For details, see Managing data tiering from your clusters.

Tiering data from on-premises ONTAP clusters to S3 object storage

Free space on your on-prem ONTAP clusters by tiering inactive data to any object storage service which uses the Simple Storage Service (S3) protocol.

> Customers who want to use object stores that are not officially supported as a cloud tier can do so using these instructions. Customers must test and confirm that the object store meets their requirements.
>
> NetApp does not support nor is liable for any issues arising from any third-party Object Store Service, specifically where it does not have agreed support arrangements with the third party with whom the product originated. It is acknowledged and agreed that NetApp shall not be liable for any associated damage or otherwise be required to provide support on that third-party product.

Quick start

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

1 Prepare to tier data to S3-compatible object storage

You need the following:

- An on-prem ONTAP cluster that's running ONTAP 9.8 or later, and a connection over a user-specified port to the S3-compatible object storage. Learn how to discover a cluster.
- The FQDN, Access Key, and Secret Key for the object storage server so that the ONTAP cluster can

access the bucket.

- A Connector installed on your premises.
- Networking for the Connector that enables an outbound HTTPS connection to the ONTAP cluster, to the S3-compatible object storage, and to the Cloud Tiering service.

2 Set up tiering

In Cloud Manager, select an on-prem working environment, click **Enable** for the Tiering service, and follow the prompts to tier data to S3-compatible object storage.

3 Set up licensing

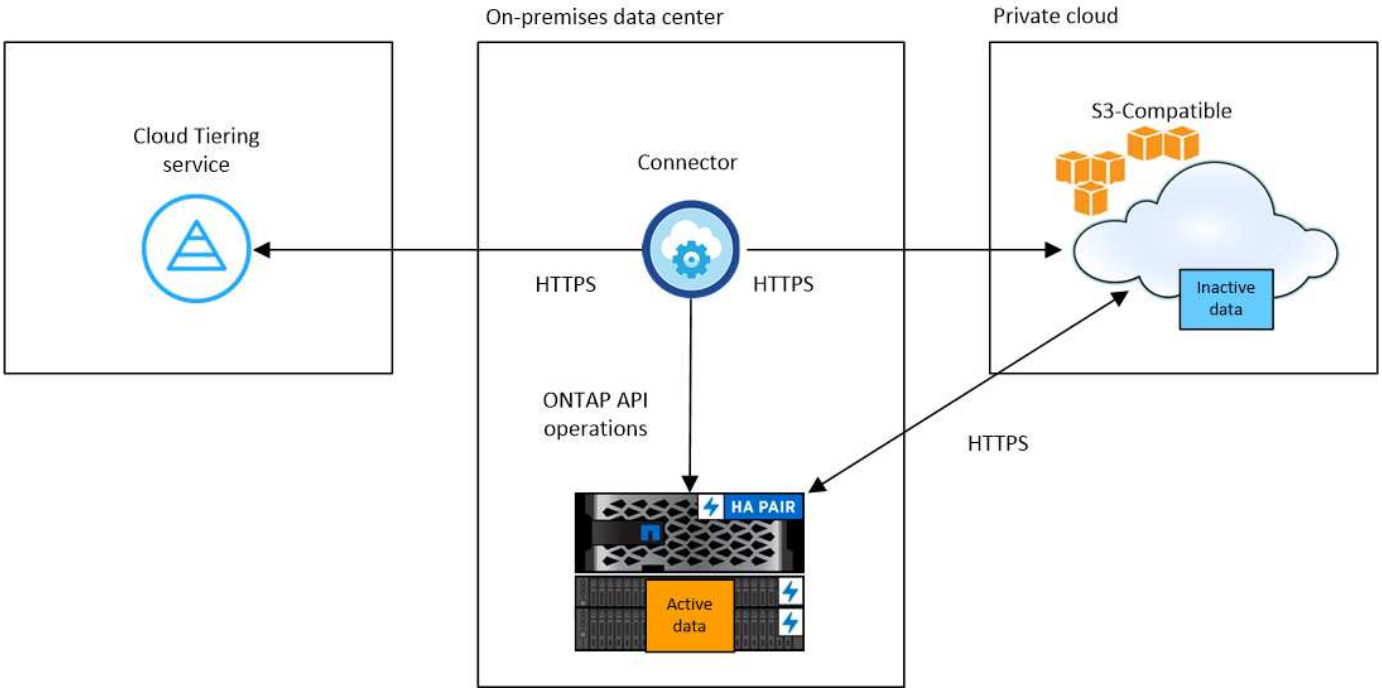
Pay for Cloud Tiering through a pay-as-you-go subscription from your cloud provider, a NetApp Cloud Tiering bring-your-own-license, or a combination of both:

- To subscribe to the Cloud Manager PAYGO offering from the AWS Marketplace, Azure Marketplace, or GCP Marketplace, click **Subscribe** and follow the prompts.
- To pay using a Cloud Tiering BYOL license, contact us if you need to purchase one, and then add it to your account from the Cloud Manager Digital Wallet.

Requirements

Verify support for your ONTAP cluster, set up your networking, and prepare your object storage.

The following image shows each component and the connections that you need to prepare between them:



Communication between the Connector and the S3-compatible object storage server is for object storage setup only.

Preparing your ONTAP clusters

Your ONTAP clusters must meet the following requirements when tiering data to S3-compatible object storage.

Supported ONTAP platforms

You can tier data from AFF systems, or FAS systems with all-SSD aggregates or all-HDD aggregates.

Supported ONTAP version

ONTAP 9.8 or later

Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over a user-specified port to S3-compatible object storage (the port is configurable during tiering setup).

  ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

- An inbound connection is required from the Connector, which must reside on your premises.

  A connection between the cluster and the Cloud Tiering service is not required.

- An intercluster LIF is required on each ONTAP node that hosts the volumes you want to tier. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage.

  When you set up data tiering, Cloud Tiering prompts you for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created. Learn more about LIFs and IPspaces.

Supported volumes and aggregates

The total number of volumes that Cloud Tiering can tier might be less than the number of volumes on your ONTAP system. That's because volumes can't be tiered from some aggregates. Refer to ONTAP documentation for functionality or features not supported by FabricPool.

Cloud Tiering supports both FlexVol and FlexGroup volumes.

Discovering an ONTAP cluster

You need to create an on-prem ONTAP working environment in the Cloud Manager Canvas before you can start tiering cold data.

Learn how to discover a cluster.

Preparing S3-compatible object storage

S3-compatible object storage must meet the following requirements.

S3 credentials

When you set up tiering to S3-compatible object storage, you're prompted to create an S3 bucket or to select an existing S3 bucket. You need to provide Cloud Tiering with an S3 access key and secret key. Cloud Tiering uses the keys to access your bucket.

These access keys must be associated with a user who has the following permissions:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Creating or switching Connectors

A Connector is required to tier data to the cloud. When tiering data to S3-compatible object storage, a Connector must be available on your premises. You'll either need to install a new Connector or make sure that the currently selected Connector resides on-prem.

- Learn about Connectors
- Installing the Connector on a Linux host
- Switching between Connectors

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

1. Ensure that the network where the Connector is installed enables the following connections:
    - An outbound internet connection to the Cloud Tiering service over port 443 (HTTPS)
    - An HTTPS connection over port 443 to S3-compatible object storage
    - An HTTPS connection over port 443 to your ONTAP cluster management LIF

Tiering inactive data from your first cluster to S3-compatible object storage

After you prepare your environment, start tiering inactive data from your first cluster.

What you'll need

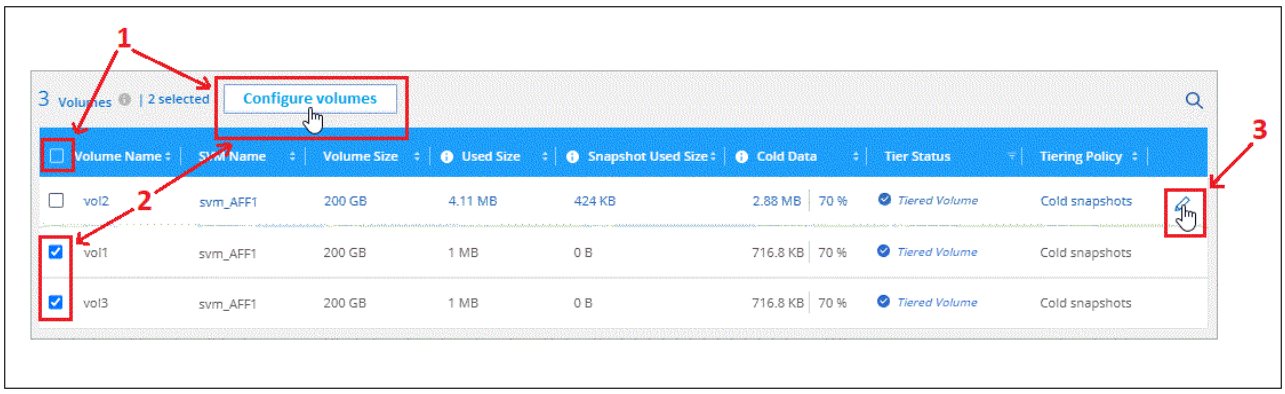
- An on-premises working environment.
- The FQDN of the S3-compatible object storage server and the port that will be used for HTTPS communications.
- An access key and secret key that has the required S3 permissions.

Steps

1. Select an on-prem cluster.
2. In the right panel, click **Enable** for the Tiering service.

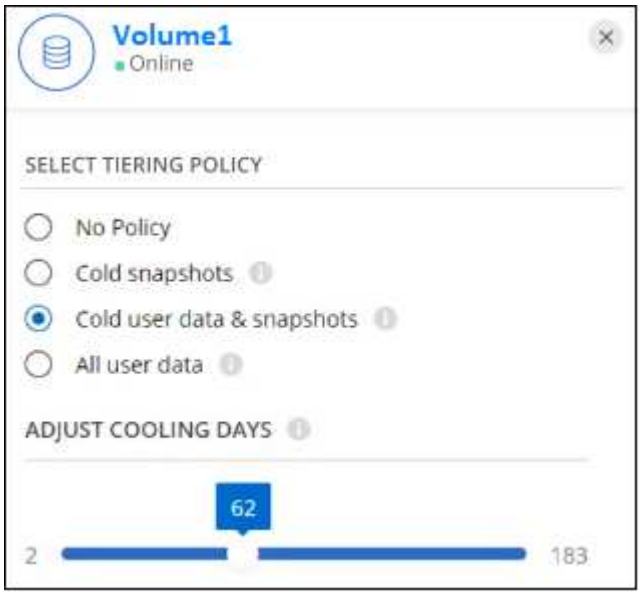
3. **Choose your provider**: Select **S3 Compatible** and click **Continue**.
4. Complete the steps on the **Tiering Setup** page:
   a. **Server**: Enter the FQDN of the S3-compatible object storage server, the port that ONTAP should use for HTTPS communication with the server, and the access key and secret key for an account that has the required S3 permissions.
   b. **Bucket**: Add a new bucket or select an existing bucket and click **Continue**.
   c. **Cluster Network**: Select the IPspace that ONTAP should use to connect to object storage and click **Continue**.

      Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your S3-compatible object storage.
5. On the *Success* page click **Continue** to set up your volumes now.
6. On the *Tier Volumes* page, select the volumes that you want to configure tiering for and click **Continue**:
   - To select all volumes, check the box in the title row (Volume Name) and click **Configure volumes**.
   - To select multiple volumes, check the box for each volume (Volume_1) and click **Configure volumes**.
   - To select a single volume, click the row (or icon) for the volume.



7. In the *Tiering Policy* dialog, select a tiering policy, optionally adjust the cooling days for the selected volumes, and click **Apply**.

   Learn more about volume tiering policies and cooling days.



Result

You've successfully set up data tiering from volumes on the cluster to S3-compatible object storage.

What's next?

Be sure to subscribe to the Cloud Tiering service.

You can add additional clusters or review information about the active and inactive data on the cluster. For details, see Managing data tiering from your clusters.

Set up licensing for Cloud Tiering

A 30-day free trial of Cloud Tiering starts when you set up tiering from your first cluster. After the free trial ends, you'll need to pay for Cloud Tiering through a pay-as-you-go Cloud Manager subscription from your cloud provider's marketplace, a BYOL license from NetApp, or a combination of both.

A few notes before you read any further:

- If you've already subscribed to the Cloud Manager subscription (PAYGO) in your cloud provider's marketplace, then you're automatically subscribed to Cloud Tiering from on-premises ONTAP systems as well. You'll see an active subscription in the Cloud Tiering **Licensing** tab. You won't need to subscribe again.
- The BYOL Cloud Tiering license is a *floating* license that you can use across multiple on-premises ONTAP clusters in your Cloud Manager account. This is different than in the past where you purchased a *FabricPool* license for each cluster.
- There are no charges when tiering data to StorageGRID, so neither a BYOL license or PAYGO registration is required. This tiered data doesn't count against the capacity purchased in your license.

Learn more about how licensing works for Cloud Tiering.

Use a Cloud Tiering PAYGO subscription

Pay-as-you-go subscriptions from your cloud provider's marketplace enable you to license the use of Cloud Volumes ONTAP systems and many Cloud Data Services, such as Cloud Tiering.

Subscribing from the AWS Marketplace

Subscribe to Cloud Tiering from the AWS Marketplace to set up a pay-as-you-go subscription for data tiering from ONTAP clusters to AWS S3.

Steps

1. In Cloud Manager, click **Tiering > Licensing**.
2. Click **Subscribe** under AWS Marketplace and then click **Continue**.
3. Subscribe from the AWS Marketplace, and then log back in to Cloud Central to complete the registration.

   The following video shows the process:

   ► https://docs.netapp.com/us-en/cloud-manager-tiering//media/video_subscribing_aws_tiering.mp4 *(video)*

Subscribing from the Azure Marketplace

Subscribe to Cloud Tiering from the Azure Marketplace to set up a pay-as-you-go subscription for data tiering from ONTAP clusters to Azure Blob storage.

Steps

1. In Cloud Manager, click **Tiering > Licensing**.
2. Click **Subscribe** under Azure Marketplace and then click **Continue**.
3. Subscribe from the Azure Marketplace, and then log back in to Cloud Central to complete the registration.

   The following video shows the process:

   ► https://docs.netapp.com/us-en/cloud-manager-tiering//media/video_subscribing_azure_tiering.mp4

(video)

Subscribing from the GCP Marketplace

Subscribe to Cloud Tiering from the GCP Marketplace to set up a pay-as-you-go subscription for data tiering from ONTAP clusters to Google Cloud storage.

Steps

1. In Cloud Manager, click **Tiering > Licensing**.
2. Click **Subscribe** under GCP Marketplace and then click **Continue**.
3. Subscribe from the GCP Marketplace, and then log back in to Cloud Central to complete the registration.

   The following video shows the process:

   ► https://docs.netapp.com/us-en/cloud-manager-tiering//media/video_subscribing_gcp_tiering.mp4 *(video)*

Use a Cloud Tiering BYOL license

Bring-your-own licenses from NetApp provide 2-, 12-, 24-, or 36-month terms. The BYOL **Cloud Tiering** license is a *floating* license that you can use across multiple on-premises ONTAP clusters in your Cloud Manager account. The total tiering capacity defined in your Cloud Tiering license is shared among **all** of your on-prem clusters, making initial licensing and renewal easy.

If you don't have a Cloud Tiering license, contact us to purchase one:

- Send email to purchase a license.
- Click the chat icon in the lower-right of Cloud Manager to request a license.

Optionally, if you have an unassigned node-based license for Cloud Volumes ONTAP that you won't be using, you can convert it to a Cloud Tiering license with the same dollar-equivalence and the same expiration date. Go here for details.

You use the Digital Wallet page in Cloud Manager to manage Cloud Tiering BYOL licenses. You can add new licenses and update existing licenses.

New Cloud Tiering BYOL licensing starting August 21, 2021

The new **Cloud Tiering** license was introduced in August 2021 for tiering configurations that are supported within Cloud Manager using the Cloud Tiering service. Cloud Manager currently supports tiering to the following cloud storage: Amazon S3, Azure Blob storage, Google Cloud Storage, S3-compatible object storage, IBM Cloud Object Storage, and StorageGRID.

The **FabricPool** license that you may have used in the past to tier on-premises ONTAP data to the cloud is being retained only for ONTAP deployments in sites that have no internet access (also known as "dark sites") or for MetroCluster systems using FabricPool Mirror. If you are using these configurations, you'll install a FabricPool license on each cluster using System Manager or the ONTAP CLI.

Note that tiering to StorageGRID does not require a FabricPool or Cloud Tiering license.

If you are currently using FabricPool licensing, you're not affected until your FabricPool license reaches its expiration date or maximum capacity. Contact NetApp when you need to update your license, or earlier to make sure there is no interruption in your ability to tier data to the cloud.

- If you're using a configuration that's supported in Cloud Manager, your FabricPool licenses will be converted to Cloud Tiering licenses and they'll appear in the Digital Wallet. When those initial licenses expire, you'll need to update the Cloud Tiering licenses.
- If you're using a configuration that's not supported in Cloud Manager, then you'll continue using a FabricPool license. See how to license tiering using System Manager.

Here are some things you need to know about the two licenses:

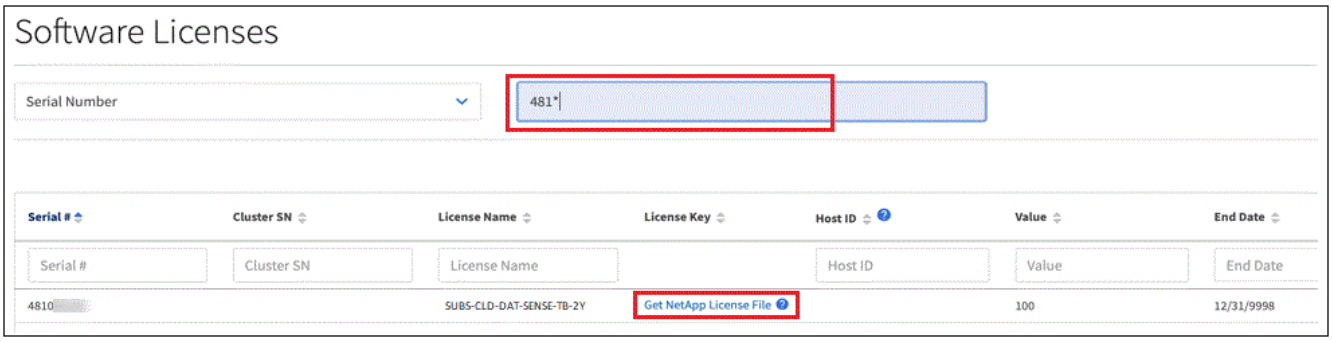
Cloud Tiering license	FabricPool license
It is a *floating* license that you can use across multiple on-premises ONTAP clusters.	It is a per-cluster license that you purchase and license for *every* cluster.
It is registered in Cloud Manager in the Digital Wallet.	It is applied to individual clusters using System Manager or the ONTAP CLI.
Tiering configuration and management is done through the Cloud Tiering service in Cloud Manager.	Tiering configuration and management is done through System Manager or the ONTAP CLI.
Once configured, you can use the tiering service without a license for 30 days using the free trial.	Once configured, you can tier the first 10 TB of data for free.

Obtain your Cloud Tiering license file

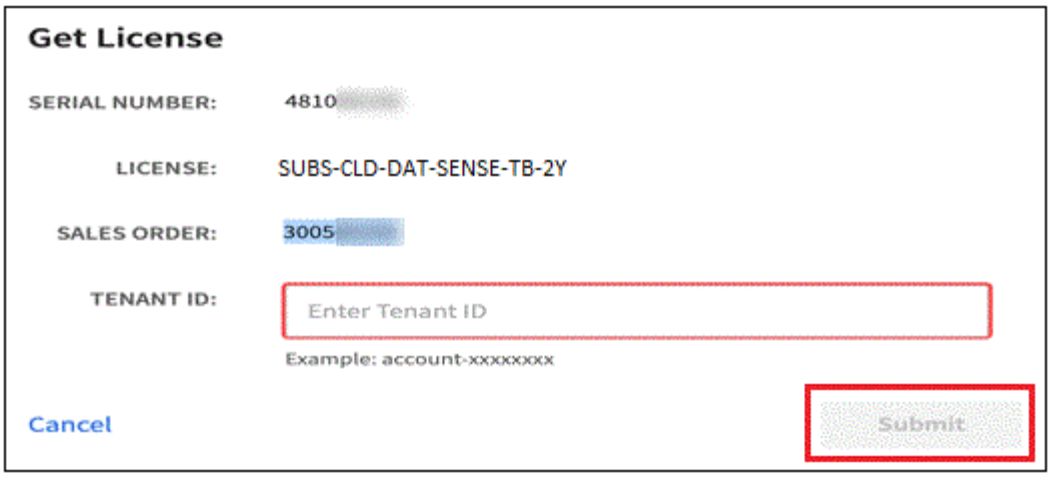
After you have purchased your Cloud Tiering license, you activate the license in Cloud Manager by entering the Cloud Tiering serial number and NSS account, or by uploading the NLF license file. The steps below show how to get the NLF license file if you plan to use that method.

Steps

1. Sign in to the NetApp Support Site and click **Systems > Software Licenses**.
2. Enter your Cloud Tiering license serial number.



3. Under **License Key**, click **Get NetApp License File**.
4. Enter your Cloud Manager Account ID (this is called a Tenant ID on the support site) and click **Submit** to download the license file.



You can find your Cloud Manager Account ID by selecting the **Account** drop-down from the top of Cloud Manager, and then clicking **Manage Account** next to your account. Your Account ID is in the Overview tab.

Add Cloud Tiering BYOL licenses to your account

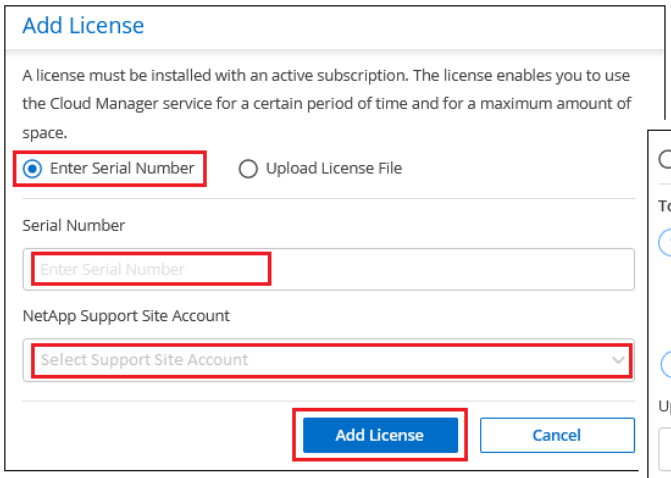
After you purchase a Cloud Tiering license for your Cloud Manager account, you need to add the license to Cloud Manager to use the Cloud Tiering service.

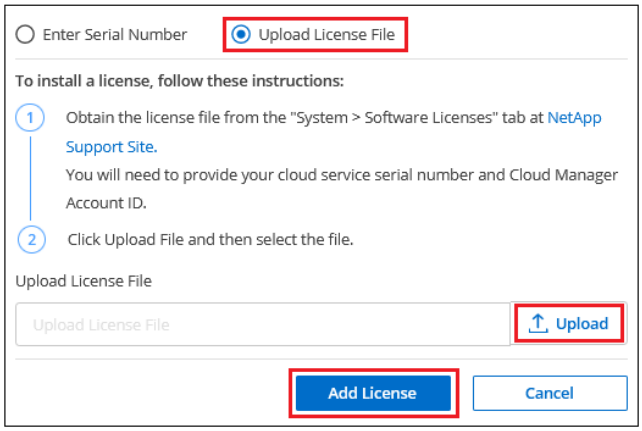
Steps

1. Click **All Services > Digital Wallet > Data Services Licenses**.
2. Click **Add License**.
3. In the *Add License* dialog, enter the license information and click **Add License**:
   - If you have the tiering license serial number and know your NSS account, select the **Enter Serial Number** option and enter that information.

     If your NetApp Support Site account isn't available from the drop-down list, add the NSS account to Cloud Manager.

   - If you have the tiering license file, select the **Upload License File** option and follow the prompts to attach the file.





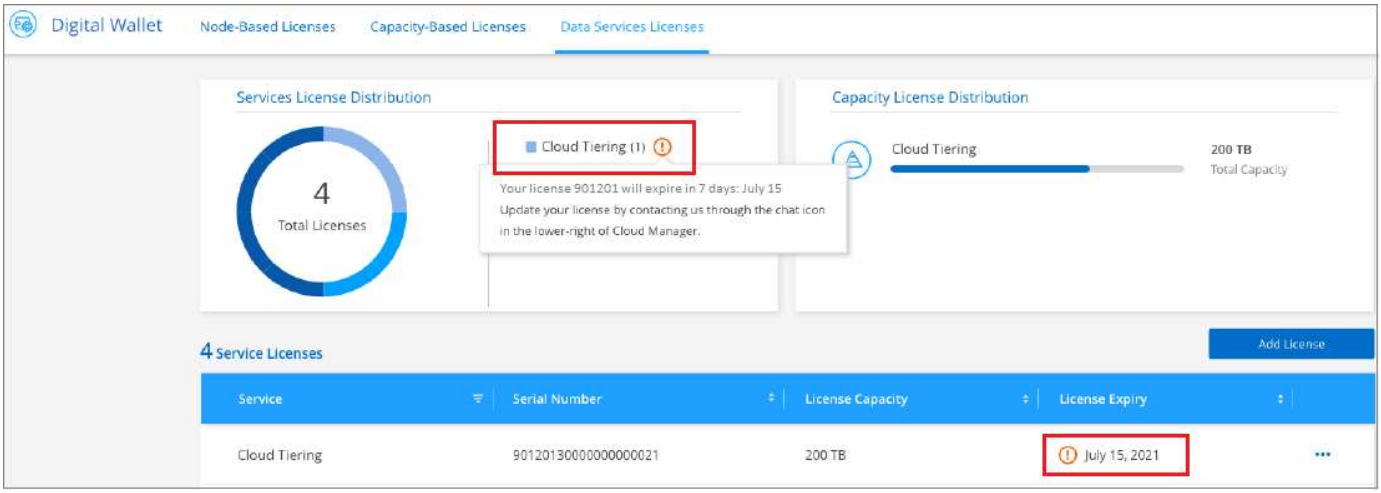
Result

Cloud Manager adds the license so that your Cloud Tiering service is active.

Update a Cloud Tiering BYOL license

If your licensed term is nearing the expiration date, or if your licensed capacity is reaching the limit, you'll be notified in Cloud Tiering.

This status also appears in the Digital Wallet page.



You can update your Cloud Tiering license before it expires so that there is no interruption in your ability to tier your data to the cloud.

Steps

1. Click the chat icon in the lower-right of Cloud Manager to request an extension to your term or additional capacity to your Cloud Tiering license for the particular serial number.

   After you pay for the license and it is registered with the NetApp Support Site, Cloud Manager automatically updates the license in the Digital Wallet and the Data Services Licenses page will reflect the change in 5 to 10 minutes.

2. If Cloud Manager can't automatically update the license, then you'll need to manually upload the license file.

   a. You can obtain the license file from the NetApp Support Site.

   b. On the Digital Wallet page in the *Data Services Licenses* tab, click ••• for the service serial number you are updating, and click **Update License**.

c. In the *Update License* page, upload the license file and click **Update License**.

Result

Cloud Manager updates the license so that your Cloud Tiering service continues to be active.

Apply Cloud Tiering licenses to clusters in special configurations

ONTAP clusters in the following configurations can use Cloud Tiering licenses, but the license must be applied in a different manner than typical single-node and HA-configured ONTAP clusters:

- Clusters in Tiering Mirror configurations (clusters connected to two object stores)

  MetroCluster configurations using FabricPool Mirror are not currently supported

- Clusters that are tiered to IBM Cloud Object Storage

Process for existing clusters that have a FabricPool license

When you discover any of these special cluster types in Cloud Tiering, Cloud Tiering recognizes the FabricPool license and adds the license into the Digital Wallet. Those clusters will continue tiering data as usual. When the FabricPool license expires, you'll need to purchase a Cloud Tiering license.

Process for newly created clusters

When you discover typical clusters in Cloud Tiering, you'll configure tiering using the Cloud Tiering interface. In these cases the following actions happen:

1. The "parent" Cloud Tiering license tracks the capacity being used for tiering by all clusters to make sure there is enough capacity in the license
2. A "child" tiering license is automatically installed on each cluster to communicate with the "parent" license in the Digital Wallet

For the two configurations listed above, you'll need to configure tiering using System Manager or the ONTAP CLI (not by using the Cloud Tiering interface). So in these cases you'll need to push the "child" license to these clusters manually from the Cloud Tiering interface.

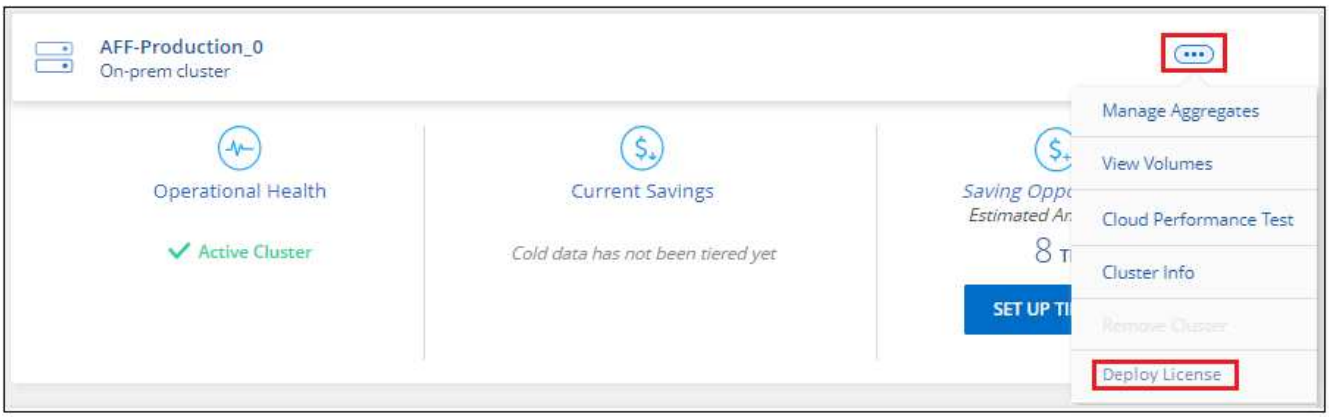
Since data is tiered to two different object storage locations for Tiering Mirror configurations, you'll need to purchase a license with enough capacity for tiering to both locations.

Steps

1. Install and configure your ONTAP clusters using System Manager or the ONTAP CLI.

Do not configure tiering at this point.

2. Purchase a Cloud Tiering license for the capacity needed for the new cluster, or clusters.
3. In Cloud Manager, add the license to the Digital Wallet.
4. In Cloud Tiering, discover the new clusters.
5. From the Cluster Dashboard, click ••• for the cluster and select **Deploy License**.



6. In the *Deploy License* dialog, click **Deploy**.

   The child license is deployed to the ONTAP cluster.

7. Return to System Manager or the ONTAP CLI and set up your tiering configuration.

   FabricPool Mirror configuration information

   Tiering to IBM Cloud Object Storage information

Cloud Tiering technical FAQ

This FAQ can help if you're just looking for a quick answer to a question.

Cloud Tiering service

The following FAQs relate to how Cloud Tiering works.

What are the benefits of using the Cloud Tiering service?

Cloud Tiering addresses the challenges that come with rapid data growth, providing you with benefits such as:

- Effortless data center extension to the cloud, providing up to 50x more space
- Storage optimization, yielding an average storage savings of 70%
- Reduced total cost of ownership by 30%, on average
- No need to refactor applications

What kind of data is useful to tier to the cloud?

Essentially, any data that is considered inactive on both primary and secondary storage systems is a good target to move to the cloud. On primary systems, such data can include snapshots, historical records, and

finished projects. On secondary systems, this includes all volumes that contain copies of primary data made for DR and backup purposes.

Can I tier data from both NAS volumes and SAN volumes?

Yes, you can tier data from NAS volumes to the public cloud or to private clouds, like StorageGRID. When tiering data that is accessed by SAN protocols, NetApp recommends using private clouds because SAN protocols are more sensitive to connectivity issues than NAS.

What is the definition of inactive data or infrequently used data, and how is that controlled?

The definition of what can also be referred to cold data is: "volume blocks (metadata excluded) that have not been accessed for some amount of time". The “amount of time” is determined by a tiering policy attribute named cooling-days.

Will Cloud Tiering retain my storage efficiency savings in the cloud tier?

Yes, the ONTAP volume-level storage efficiencies such as compression, deduplication, and compaction are preserved when moving data to the cloud tier.

What is the difference between FabricPool and Cloud Tiering?

FabricPool is ONTAP’s tiering technology that can be self-managed through the ONTAP CLI and System Manager, or managed as-a-service through Cloud Tiering. Cloud Tiering turns FabricPool into a managed service with advanced automation processes, on both ONTAP and in the cloud, providing greater visibility and control over tiering across hybrid and multi-cloud deployments.

Can the data tiered to the cloud be used for disaster recovery or for backup/archive?

No. Since the volume’s metadata is never tiered from the performance tier, the data stored in object storage cannot be accessed directly.

However, Cloud Tiering can be used to achieve cost-effective backup and DR by enabling it on secondary systems and SnapMirror destination volumes (DP volumes), to tier off all of the data (metadata excluded), thus reducing your data center footprint and TCO.

Is Cloud Tiering applied at the volume or aggregate level?

Cloud Tiering is enabled at the volume level by associating a tiering policy with each volume. Cold data identification is done at the block level.

How does Cloud Tiering determine which blocks to tier to the cloud?

The tiering policy associated with the volume is the mechanism that controls which blocks are tiered and when. The policy defines the type of data blocks (snapshots, user data, or both) and the cooling period. See Volume Tiering Policies for details.

Does Cloud Tiering enable Inactive Data Reporting?

Yes, Cloud Tiering enables Inactive Data Reporting (IDR) on each aggregate. This setting enables us to identify the amount of inactive data that can be tiered to low-cost object storage.

How long does it take IDR to show information from the moment I start running it?

IDR starts showing information after the configured cooling period has passed. Using ONTAP 9.7 and earlier, IDR had a non-adjustable cooling period of 31 days. Starting with ONTAP 9.8, the IDR cooling-period can be configured up to 183 days.

Licenses and Costs

The following FAQs relate to licensing and costs to use Cloud Tiering.

How much does using Cloud Tiering cost?

When tiering cold data to the public cloud:

- For the pay-as-you-go (PAYGO), usage-based subscription: $0.05 per GB/Month.
- For the annual (BYOL), term-based subscription: starting from $0.033 per GB/Month.

When tiering cold data to a NetApp StorageGRID system (private cloud) there is no cost.

Can I have both a BYOL and PAYGO license for the same ONTAP cluster?

Yes. Cloud Tiering allows you to use a BYOL license, a PAYGO subscription, or a combination of both.

What happens if I have reached the BYOL capacity limit?

If you reach a BYOL capacity limit, tiering of new cold data stops while all previously tiered data remains accessible. If you have a PAYGO marketplace subscription to the *Cloud Manager - Deploy & Manage Cloud Data Services*, new cold data will continue to be tiered to object storage and the charges would incur on a per-use basis.

Does the Cloud Tiering license include the egress charges from the cloud provider?

No, it does not.

Is rehydration of on-prem systems subject to the egress cost charged by the cloud providers?

Yes. All reads from the public cloud are subject to egress fees.

How can I estimate my cloud charges? Is there a “what if” mode for Cloud Tiering?

The best way to estimate how much a cloud provider will charge for hosting your data is to use their calculators: AWS, Azure and Google Cloud.

Are there any extra charges by the cloud providers for reading/retrieving data from the object storage to the on-prem storage?

Yes. Check Amazon S3 Pricing, Block Blob Pricing, and Cloud Storage Pricing for additional pricing incurred with data reading/retrieving.

How can I estimate my volumes’ savings and get a cold data report before I enable Cloud Tiering?

To get an estimate, simply add your ONTAP cluster to Cloud Manager and inspect it through the Cloud Tiering Clusters Dashboard, which is located in the Tiering tab. When Inactive Data Reporting (IDR) is disabled or has not yet been activated for a long enough period of time, Cloud Tiering uses an industry-constant of 70% to

calculate the estimated savings. Once IDR data is available, Cloud Tiering updates the savings to accurate figures.

ONTAP

The following questions relate to ONTAP.

Which ONTAP versions does Cloud Tiering support?

Cloud Tiering supports ONTAP version 9.2 and higher.

What types of ONTAP systems are supported?

Cloud Tiering is supported from single-node and high-availability AFF, FAS, and ONTAP Select clusters.

Clusters in FabricPool Mirror configurations are also supported, but the tiering configuration must be done using System Manager or the ONTAP CLI.

Can I tier data from FAS systems with HDDs only?

Yes, starting ONTAP 9.8 you can tier data from volumes hosted on HDD aggregates.

Can I tier data from an AFF joined to a cluster that has FAS nodes with HDDs?

Yes. Cloud Tiering can be configured to tier volumes hosted on any aggregate. The data tiering configuration is irrelevant to the type of controller used and whether the cluster is heterogeneous or not.

What about Cloud Volumes ONTAP?

If you have Cloud Volumes ONTAP systems, you'll find them in the Cloud Tiering Cluster Dashboard so you get a full view of data tiering in your hybrid cloud infrastructure. However, Cloud Volumes ONTAP systems are read-only from Cloud Tiering. You can't set up data tiering on Cloud Volumes ONTAP from Cloud Tiering. You set up tiering for Cloud Volumes ONTAP from the working environment in Cloud Manager.

What other requirements are necessary for my ONTAP clusters?

It depends on where you tier the cold data. Refer to the following links for more details:

- Tiering data to Amazon S3
- Tiering data to Azure Blob storage
- Tiering data to Google Cloud Storage
- Tiering data to StorageGRID
- Tiering data to S3 object storage

Object storage

The following questions relate to object storage.

Which object storage providers are supported?

Cloud Tiering supports the following object storage providers:

- Amazon S3
- Microsoft Azure Blob
- Google Cloud Storage
- NetApp StorageGRID
- S3-compatible object storage
- IBM Cloud Object Storage (the FabricPool configuration must be done using System Manager or the ONTAP CLI)

Can I use my own bucket/container?

Yes, you can. When you set up data tiering, you have the choice to add a new bucket/container or to select an existing bucket/container.

Which regions are supported?

- Supported AWS regions
- Supported Azure regions
- Supported Google Cloud regions

Which S3 storage classes are supported?

Cloud Tiering supports data tiering to the *Standard*, *Standard-Infrequent Access*, *One Zone-Infrequent Access*, *Intelligent Tiering*, and *Glacier Instant Retrieval* storage classes. See Supported S3 storage classes for more details.

Why are Amazon S3 Glacier Flexible and S3 Glacier Deep Archive not supported by Cloud Tiering?

The main reason Amazon S3 Glacier Flexible and S3 Glacier Deep Archive aren't supported is that Cloud Tiering is designed as a high-performance tiering solution, so data must be continuously available and quickly accessible for retrieval. With S3 Glacier Flexible and S3 Glacier Deep Archive, data retrieval can last anywhere between a few minutes to 48 hours.

Can I use other S3-compatible object storage services, such as Wasabi, with Cloud Tiering?

Yes, configuring S3-compatible object storage through the Tiering UI is supported for clusters using ONTAP 9.8 and later. See the details here.

Which Azure Blob access tiers are supported?

Cloud Tiering supports data tiering to the *Hot* or *Cool* access tiers for your inactive data. See Supported Azure Blob access tiers for more details.

Which storage classes are supported for Google Cloud Storage?

Cloud Tiering supports data tiering to the *Standard*, *Nearline*, *Coldline*, and *Archive* storage classes. See Supported Google Cloud storage classes for more details.

Does Cloud Tiering use one object store for the entire cluster or one per aggregate?

One object store for the entire cluster.

Can multiple buckets be attached to the same aggregate?

It is possible to attach up to two buckets per aggregate for the purpose of mirroring, where cold data is synchronously tiered to both buckets. The buckets can be from different providers and different locations. However, configuration through the Cloud Tiering UI is not supported at this time — setup is available through System Manager or the CLI.

Can different buckets be attached to different aggregates in the same cluster?

Yes. The general best practice is to attach a single bucket to multiple aggregates. However, when using the public cloud there is a maximum IOPS limitation for the object storage services, therefore multiple buckets must be considered. However, configuration through the Cloud Tiering UI is not supported at this time — setup is available through System Manager or the CLI.

What happens with the tiered data when you migrate a volume from one cluster to another?

When migrating a volume from one cluster to another, all the cold data is read from the cloud tier. The write location on the destination cluster depends on whether tiering was enabled and the type of tiering policy used on the source and destination volumes.

What happens with the tiered data when you move a volume from one node to another in the same cluster?

If the destination aggregate does not have an attached cloud tier, data is read from the cloud tier of the source aggregate and written entirely to the local tier of the destination aggregate. If the destination aggregate has an attached cloud tier, data is read from the cloud tier of the source aggregate and first written to the local tier of the destination aggregate, to facilitate quick cutover. Later, based on the tiering policy used, it is written to the cloud tier.

Starting with ONTAP 9.6, if the destination aggregate is using the same cloud tier as the source aggregate, the cold data does not move back to the local tier.

How can I bring my tiered data back on-prem?

Write back is generally performed on reads and depends on the tiering policy type. Prior to ONTAP 9.8, writing back of the entire volume can be done with a volume move operation. After 9.8, the Tiering UI has options to **Bring back all data** or **Bring back active file system**. See how to move data back to the performance tier.

When replacing an existing AFF/FAS controller with a new one, would the tiered data be migrated back on-prem?

No. During the “head swap” procedure, the only thing that changes is the aggregate’s ownership. In this case, it will be changed to the new controller without any data movement.

Can I use the tiered data to recover a volume or a system during a disaster recovery scenario?

No. Since the volume’s metadata is always stored on the local performance tier, if there’s a disaster and the local tier is lost, the metadata is lost as well and there is no way to reference the tiered data.

Can I use the cloud provider’s console or object storage explorers to look at the data tiered to a bucket? Can I use the data stored in the object storage directly without ONTAP?

No. The objects constructed and tiered to the cloud do not contain a single file but up to 1,024 4KB blocks from multiple files. A volume’s metadata always remains on the local tier.

Can I apply policies to my object store to move data around independent of tiering?

Yes. You can enable life cycle management so that Cloud Tiering transitions data from the default storage class/access tier to a more cost-effective tier after a certain number of days.

The life cycle rule is applied to all objects in the selected bucket for Amazon S3 and Google Cloud storage, and to all containers in the selected storage account for Azure Blob.

Connectors

The following questions relate to the Cloud Manager Connector.

What is the Connector?

The Connector is software running on a compute instance either within your cloud account, or on-premises, that enables Cloud Manager to securely manage cloud resources. To use the Cloud Tiering service, you must deploy a Connector.

Where does the Connector need to be installed?

- When tiering data to S3, the Connector can reside in an AWS VPC or on your premises.
- When tiering data to Blob storage, the Connector can reside in an Azure VNet or on your premises.
- When tiering data to Google Cloud Storage, the Connector must reside in a Google Cloud Platform VPC.
- When tiering data to StorageGRID or other S3-Compatible storage providers, the Connector must reside on your premises.

Can I deploy the Connector on-premises?

Yes. The Connector software can be downloaded and manually installed on a Linux host in your network. See how to install the Connector in your premises.

Is an account with a cloud service provider required before using Cloud Tiering?

Yes. You must have an account before you can define the object storage that you want to use. An account with a cloud storage provider is also required when setting up the Connector in the cloud on a VPC or VNet.

What are the implications if the Connector fails?

In the case of a Connector failure, only the visibility into the tiered environments is impacted. All the data is accessible and newly identified cold data is automatically tiered to object storage.

Tiering policies

What are the available tiering policies?

There are four tiering policies:

● None: Classifies all data as always hot; preventing any data from the volume being moved to object storage.
● Cold Snapshots (Snapshot-only): Only cold snapshot blocks are moved to object storage.
● Cold User Data and Snapshots (Auto): Both cold snapshot blocks and cold user data blocks are moved to object storage.
● All User Data (All): Classifies all data as cold; immediately moving the entire volume to object storage.

Learn more about Tiering Policies.

At which point is my data is considered cold?

Since data tiering is done at the block level, a data block is considered cold after it hasn't been accessed for a certain period of time, which is defined by the tiering policy's minimum-cooling-days attribute. The applicable range is 2-63 days with ONTAP 9.7 and earlier, or 2-183 days starting with ONTAP 9.8.

What is the default cooling period for data before it is tiered to the cloud tier?

The default cooling period for the Cold Snapshot policy is 2 days, while the default cooling period for Cold User Data and Snapshots is 31 days. The cooling-days parameter is not applicable to the All tiering policy.

Is all the tiered data retrieved from object storage when I do a full backup?

During full backup all the cold data is read. The retrieval of the data depends on the tiering policy used. When using the All and Cold User Data and Snapshots policies, the cold data is not written back to the performance tier. When using the Cold Snapshots policy, only in case of an old snapshot being used for the backup will its cold blocks be retrieved.

Can you choose a tiering size per volume?

No. However, you can choose which volumes are eligible for tiering, the type of data to be tiered, and its cooling period. This is done by associating a tiering policy with that volume.

Is the All User Data policy the only option for data protection volumes?

No. Data protection (DP) volumes can be associated with any of the three policies available. The type of policy used on the source and destination (DP) volumes determines the write location of the data.

Does resetting the tiering policy of a volume to None rehydrate the cold data or just prevent future cold blocks from being moved to the cloud?

No rehydration takes place when a tiering policy is reset, but it will prevent new cold blocks from being moved to the cloud tier.

After tiering data to the cloud, can I change the tiering policy?

Yes. The behavior after the change depends on the new associated policy.

What should I do if I want to ensure certain data is not moved to the cloud?

Do not associate a tiering policy with the volume containing that data.

Where is the metadata of the files stored?

The metadata of a volumes is always stored locally, on the performance tier — it is never tiered to the cloud.

Networking and security

The following questions relate to networking and security.

What are the networking requirements?

- The ONTAP cluster initiates an HTTPS connection over port 443 to your object storage provider.

  ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

- For StorageGRID, the ONTAP cluster initiates an HTTPS connection over a user-specified port to StorageGRID (the port is configurable during tiering setup).
- A Connector needs an outbound HTTPS connection over port 443 to your ONTAP clusters, to the object store, and to the Cloud Tiering service.

For more details, see:

- Tiering data to Amazon S3
- Tiering data to Azure Blob storage
- Tiering data to Google Cloud Storage
- Tiering data to StorageGRID
- Tiering data to S3 object storage

What tools can I use for monitoring and reporting in order to manage cold data stored in the cloud?

Other than Cloud Tiering, Active IQ Unified Manager and Active IQ Digital Advisor can be used for monitoring and reporting.

What are the implications if the network link to the cloud provider fails?

In case of a network failure, the local performance tier remains online and hot data remains accessible. However, blocks that were already moved to the cloud tier will be inaccessible and applications will receive an error message when trying to access that data. Once connectivity is restored, all data will be seamlessly accessible.

Is there a network bandwidth recommendation?

The underlying FabricPool tiering technology read latency depends on connectivity to the cloud tier. Although tiering works on any bandwidth, it is recommended to place intercluster LIFs on 10 Gbps ports to provide adequate performance. There are no recommendations or bandwidth limitations for the Connector.

Is there any latency when a user attempts to access tiered data?

Yes. Cloud tiers cannot provide the same latency as the local tier since latency depends on the connectivity. To estimate the latency and throughput of an object store, Cloud Tiering provides a Cloud Performance Test (based on the ONTAP object store profiler) that can be used after the object store is attached and before tiering is set up.

How is my data secured?

AES-256-GCM encryption is maintained on both the performance and cloud tiers. TLS 1.2 encryption is used to encrypt data over the wire as it moves between tiers, and to encrypt communication between the Connector and both the ONTAP cluster and the object store.

Do I need an Ethernet port installed and configured on my AFF?

Yes. An intercluster LIF must be configured on an ethernet port, on each node within an HA pair that hosts volumes with data you plan to tier to the cloud. For more information, see the Requirements section for the cloud provider where you plan to tier data.

What permissions are required?

- For Amazon, permissions are required to manage the S3 bucket.
- For Azure, no extra permissions are needed outside of the permissions that you need to provide to Cloud Manager.
- For Google Cloud, Storage Admin permissions are needed for a service account that has storage access keys.
- For StorageGRID, S3 permissions are needed.
- For S3-compatible object storage, S3 permissions are needed.

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.