Tier data to the cloud

Cloud Manager

NetApp
December 07, 2020

NetApp®

Table of Contents

Tier data to the cloud

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 a 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 data remains on high-performance SSDs, while inactive data is tiered to low-cost object storage while preserving ONTAP data efficiencies.

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

- 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

> 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.

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

> While Cloud Tiering can significantly reduce storage footprints, it is not a backup solution.

Supported object storage providers

You can tier inactive data from an ONTAP cluster to Amazon S3, Microsoft Azure Blob storage, Google Cloud Storage, or StorageGRID (private cloud).

Pricing and licenses

Pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license called *FabricPool*, 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 FabricPool 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 FabricPool 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 FabricPool 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 FabricPool license.

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

Bring your own license

Bring your own license by purchasing an ONTAP FabricPool license from NetApp. You can purchase term-based or perpetual licenses.

After you purchase a FabricPool license, you'll need to add it to the cluster, which you can do directly from Cloud Tiering.

After you activate the license through Cloud Tiering, if you purchase additional add-on capacity at a later time, the license on the cluster is automatically updated with the new capacity. There's no need to apply a new NetApp License File (NLF) to the cluster.

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

Contact us to purchase a 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:
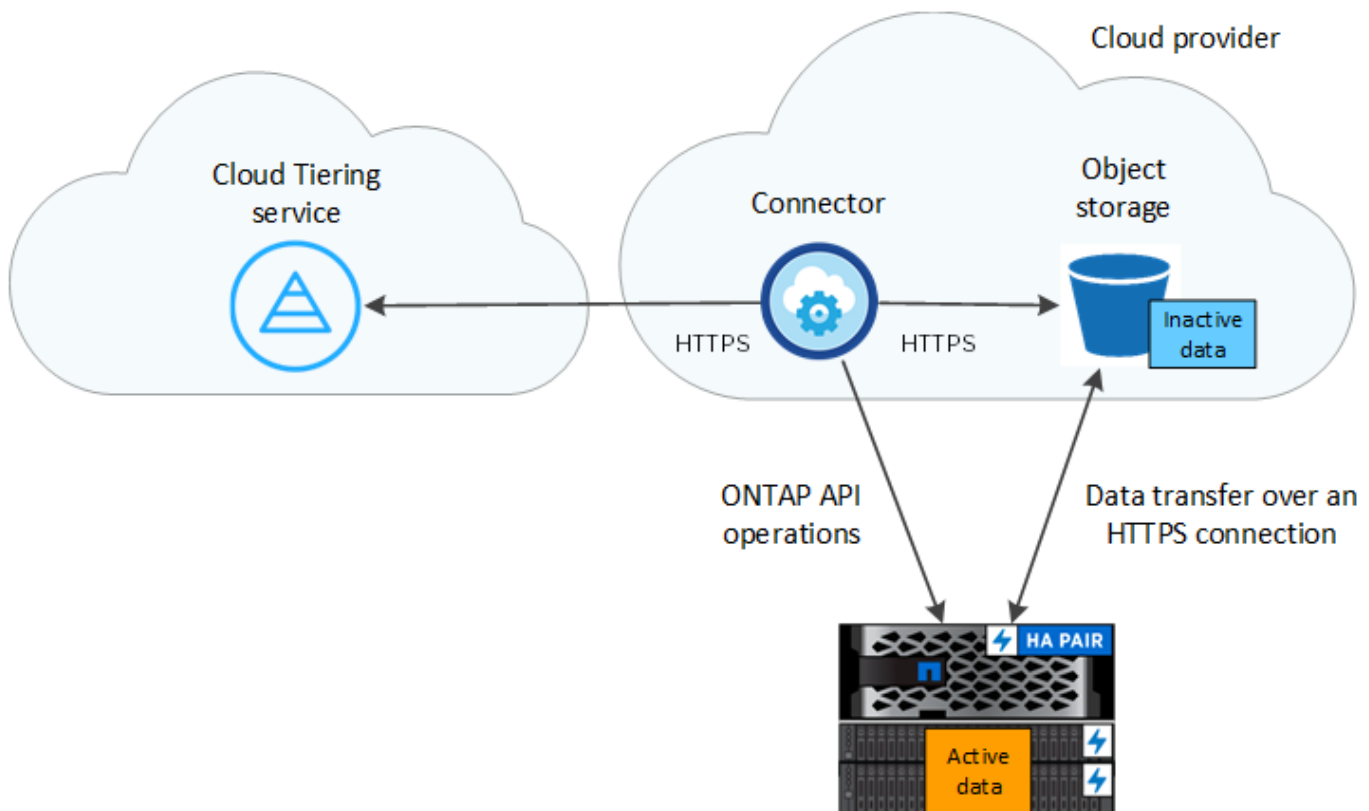
At a high level, Cloud Tiering works like this:

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 and a storage class or access tier.

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).

Object storage

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

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.

No tiering policy

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

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 the number of days.

> ⓘ Writes from the cloud tier to the performance tier are disabled if performance tier capacity is greater than 70%. If this occurs, blocks are accessed directly from the cloud tier.

Cold user data (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.

Data is tiered only after an aggregate has reached 50% capacity and when the data has reached the cooling period. The cooling period is the time that user data in a volume must remain inactive for the data to be considered "cold" and moved to the object store. The default number of cooling days is 31, but you can adjust the number of days.

> ℹ️ Writes from the cloud tier to the performance tier are disabled if performance tier capacity is greater than 70%. If this occurs, blocks are accessed directly 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.

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).

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

Get started

Tiering data from on-premises ONTAP clusters to Amazon S3

Free space on your on-prem ONTAP clusters by tiering data to Amazon S3. Data tiering is powered by NetApp's Cloud Tiering service.

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 Amazon S3**

You need the following:

- An AFF or FAS system with all-SSD aggregates that's running ONTAP 9.2 or later and has an HTTPS connection to Amazon S3.
- 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.

2 **Set up tiering**

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

3 **Set up licensing**

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

- To subscribe from the AWS Marketplace, click **Tiering** > **Licensing**, click **Subscribe**, and then follow the prompts.
- To pay using a tiering license, contact us if you need to purchase one, and then add it to your cluster from Cloud Tiering.

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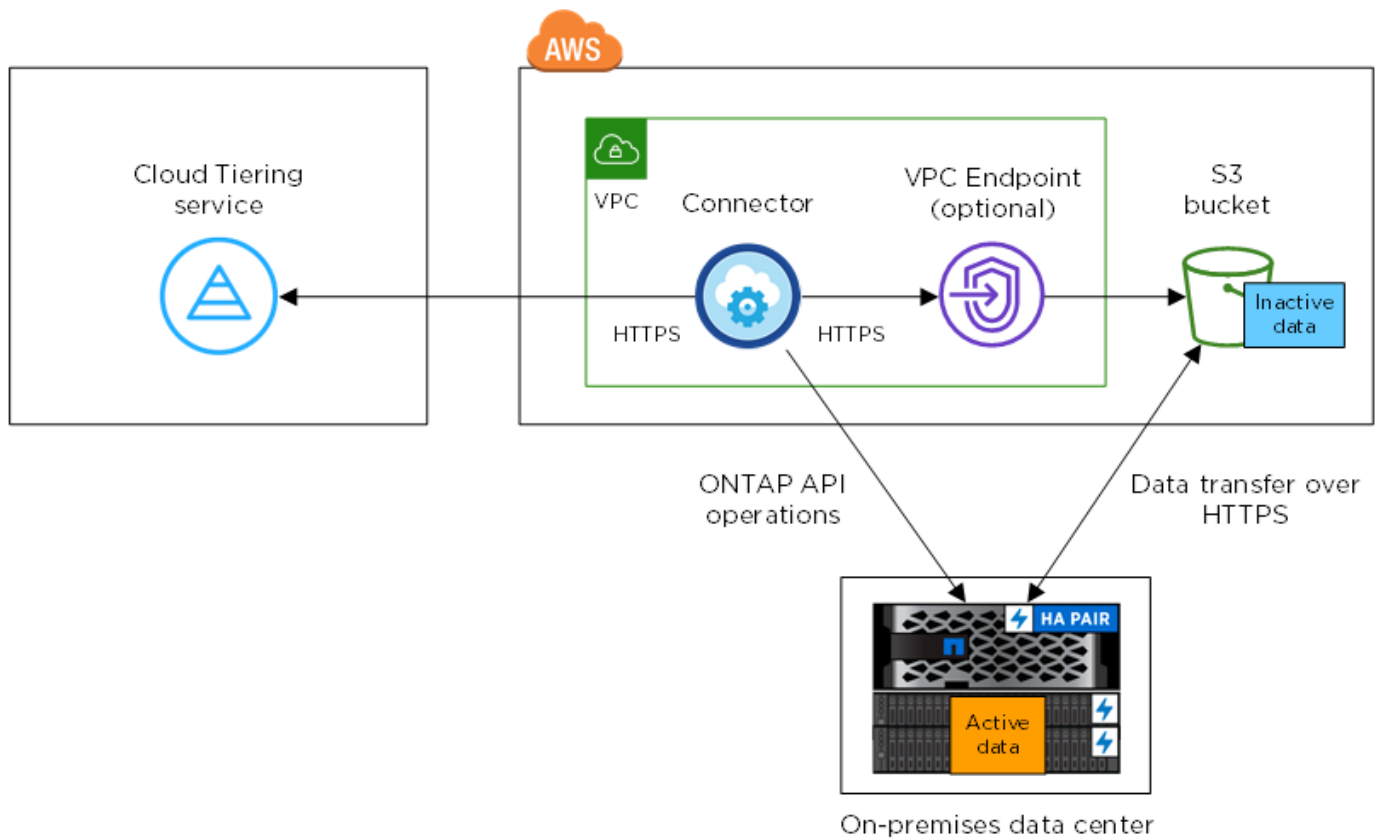
> Communication between a Connector and S3 is for object storage setup only. The Connector can reside on your premises, instead of in the cloud.

Preparing your ONTAP clusters

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

Supported ONTAP platforms

Cloud Tiering supports AFF systems and all-SSD aggregates on FAS systems.

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. Because performance is significantly better

when using AWS Direct Connect, 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 tiered volumes. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage.

  IPspaces enable network traffic segregation, allowing for separation of client traffic for privacy and security. Learn more about IPspaces.

  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.

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. For example, you can't tier data from SnapLock volumes or from MetroCluster configurations. 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.

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
- Connector host requirements
- Installing the Connector on an existing 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 clusters

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.

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.

1. Select an on-prem cluster.

2. Click **Setup Tiering**.
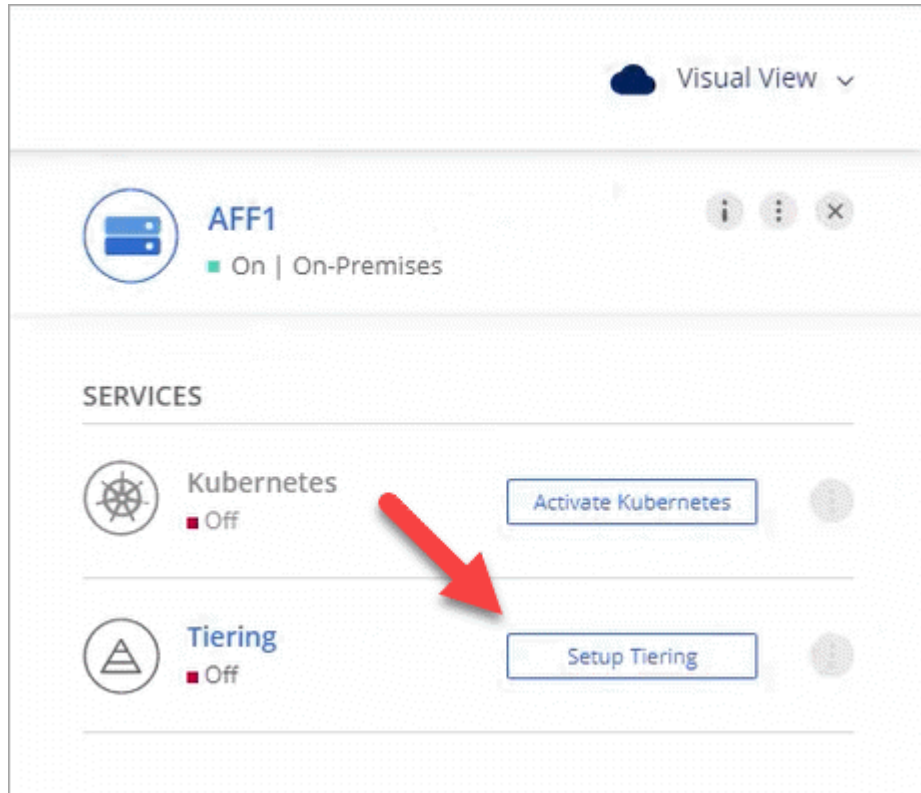
You're now on the Tiering dashboard.

3. Click **Set up Tiering** next to the cluster.

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**.

   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**: Select the S3 storage class that you want to transition the data to after 30 days and click **Continue**.

   If you choose Standard, then the data remains in that storage class.

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

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. Click **Continue** to select the volumes that you want to tier.

6. On the **Tier Volumes** page, set up tiering for each volume.

Learn more about volume tiering policies.

◦ To select a tiering policy for just one volume, click the ✏ icon, select a tiering policy, and optionally adjust the cooling days.

◦ To select a tiering policy for several volumes, select multiple volumes, click **Modify selected volumes**, select a tiering policy, and optionally adjust the 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 from 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 data to Azure Blob storage. Data tiering is powered by NetApp's Cloud Tiering service.

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 AFF or FAS system with all-SSD aggregates that's running ONTAP 9.4 or later and has an HTTPS connection to Azure Blob storage.
- A Connector installed in an Azure VNet.
- Networking for a Connector that enables an outbound HTTPS connection to the ONTAP cluster in your data center, to Azure Blob storage, and to the Cloud Tiering service.

2 **Set up tiering**

In Cloud Manager, select an on-prem working environment, click **Setup Tiering** 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 tiering license, or a combination of both:

- To subscribe from the Azure Marketplace, click **Tiering** > **Licensing**, click **Subscribe**, and then follow the prompts.
- To add a tiering license, contact us if you need to purchase one, and then add it to your cluster from Cloud Tiering.

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:

On-premises data center
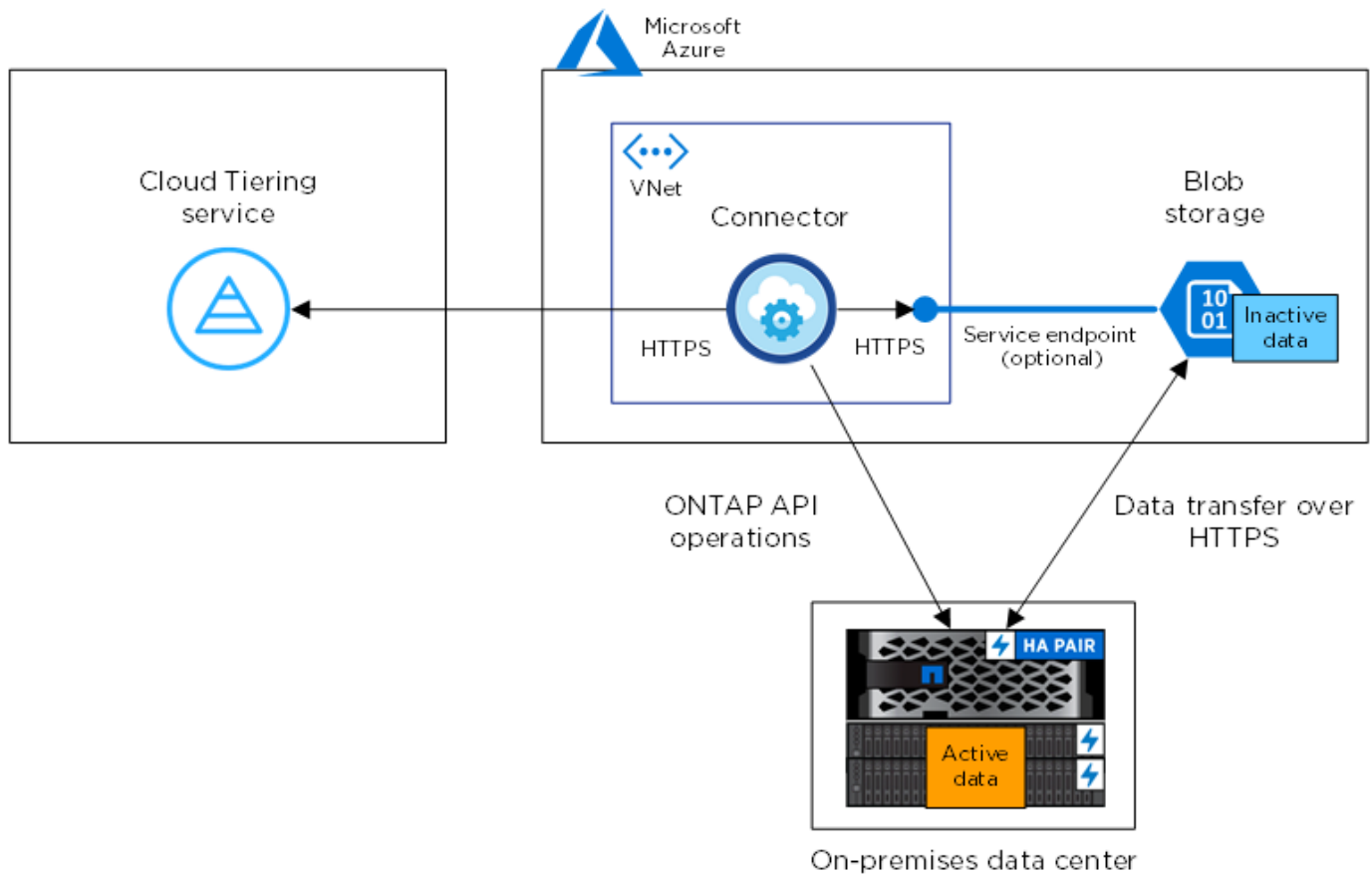
	Communication between the Connector and Blob storage is for object storage setup only.

Preparing your ONTAP clusters

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

Supported ONTAP platforms

Cloud Tiering supports AFF systems and all-SSD aggregates on FAS systems.

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. Because performance is significantly better when using ExpressRoute, doing so is the recommended best practice.

- An inbound connection is required from the NetApp Service Connector, which resides in an Azure VNet.

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

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

  IPspaces enable network traffic segregation, allowing for separation of client traffic for privacy and security. Learn more about IPspaces.

  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.

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. For example, you can't tier data from SnapLock volumes or from MetroCluster configurations. 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.

Creating or switching Connectors

A Connector is required to tier data to the cloud. When tiering data to Azure Blob storage, a Connector must be available in an Azure VNet. You'll either need to create a new Connector or make sure that the currently selected Connector resides in Azure.

- Learn about Connectors
- Creating a Connector in Azure
- Switching between Connectors

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps
1. Ensure that the VNet 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 clusters

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.

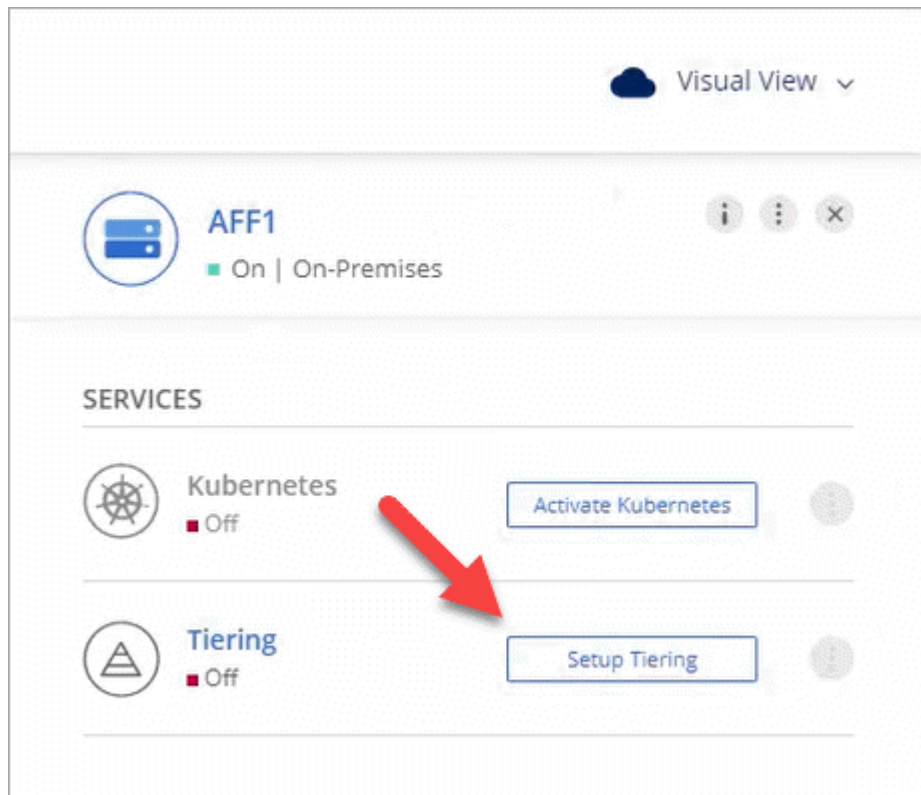**Tiering inactive data from your first cluster to Azure Blob storage**

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 **Setup Tiering**.

You're now on the Tiering dashboard.

3. Click **Set up Tiering** next to the cluster.

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.

   b. **Azure Container**: Add a new Blob container to a storage account or select an existing container and click **Continue**.

The storage account and containers that appear in this step belong to the resource group that you selected in the previous step.
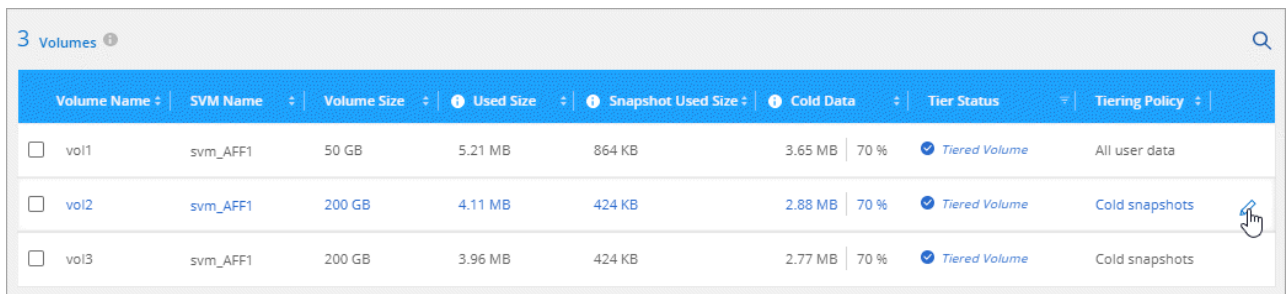
c. **Access Tier**: Select the access tier that you want to use for the tiered data and click **Continue**.

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. Click **Continue** to select the volumes that you want to tier.

6. On the **Tier Volumes** page, set up tiering for each volume.

Learn more about volume tiering policies.

◦ To select a tiering policy for just one volume, click the ✏ icon, select a tiering policy, and optionally adjust the cooling days.

◦ To select a tiering policy for several volumes, select multiple volumes, click **Modify selected volumes**, select a tiering policy, and optionally adjust the 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 from 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 data to Google Cloud Storage. Data tiering is powered by NetApp's Cloud Tiering service.

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 AFF or FAS system with all-SSD aggregates that's running ONTAP 9.6 or later and has an HTTPS connection to Google Cloud Storage.
- 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 **Setup Tiering** 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 tiering license, or a combination of both:

- To subscribe from the GCP Marketplace, click **Tiering** > **Licensing**, click **Subscribe**, and then follow the prompts.
- To add a tiering license, contact us if you need to purchase one, and then add it to your cluster from Cloud Tiering.

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:

On-premises data center
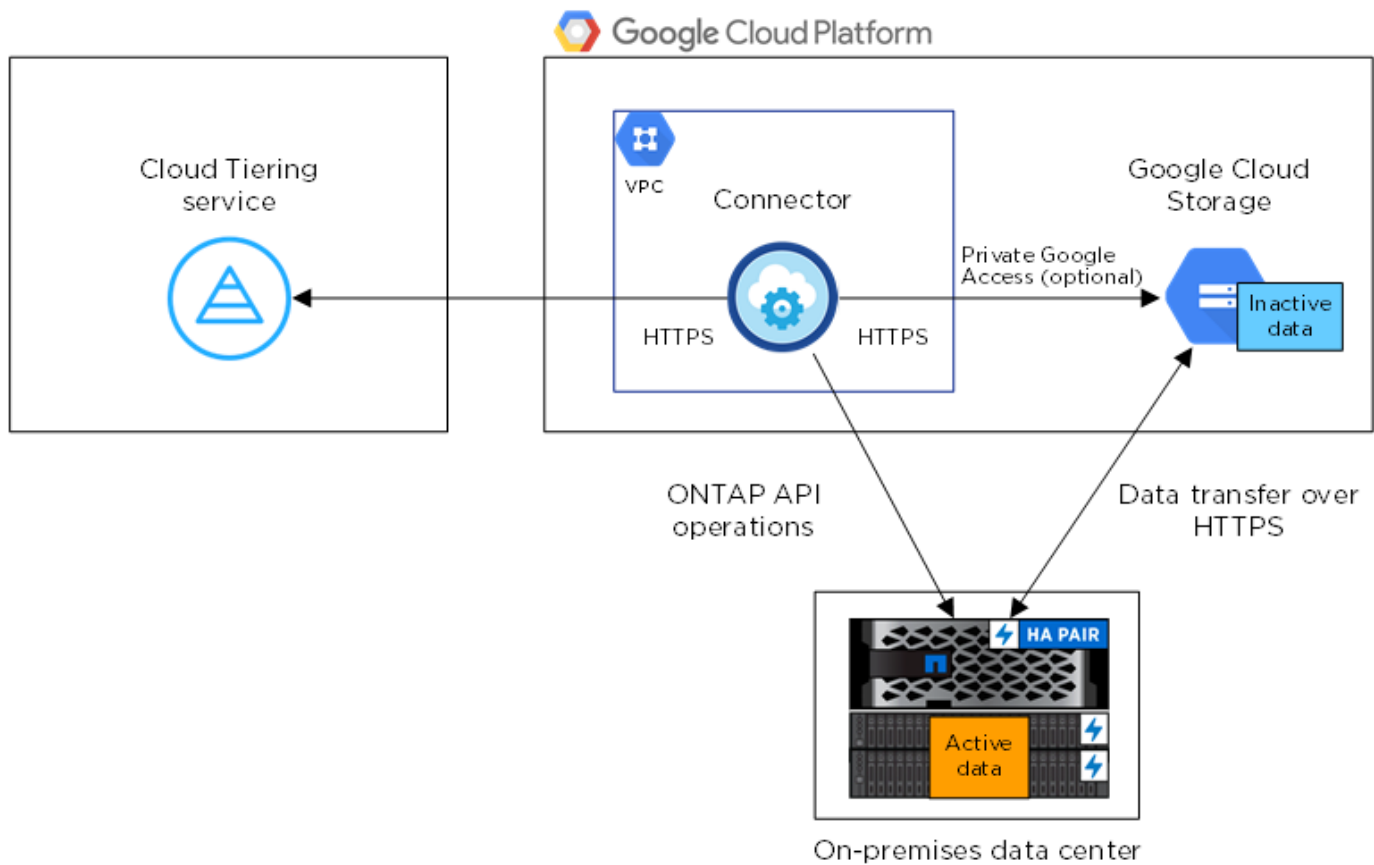
> ℹ️ Communication between the Connector and Google Cloud Storage is for object storage setup only.

Preparing your ONTAP clusters

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

Supported ONTAP platforms

Cloud Tiering supports AFF systems and all-SSD aggregates on FAS systems.

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. Because performance is significantly better when using Google Cloud Interconnect, doing so is the recommended best practice.

* An inbound connection is required from the NetApp Service Connector, which resides in an 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 tiered volumes. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage.

  IPspaces enable network traffic segregation, allowing for separation of client traffic for privacy and security. Learn more about IPspaces.

  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.

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. For example, you can't tier data from SnapLock volumes or from MetroCluster configurations. Refer to ONTAP documentation for functionality or features not supported by FabricPool.

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

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 clusters

2. Optional: Enable Private Google Access on the subnet where you plan to deploy the Service

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 for data tiering

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.

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 in Cloud Tiering later when you set up 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 **Setup Tiering**.
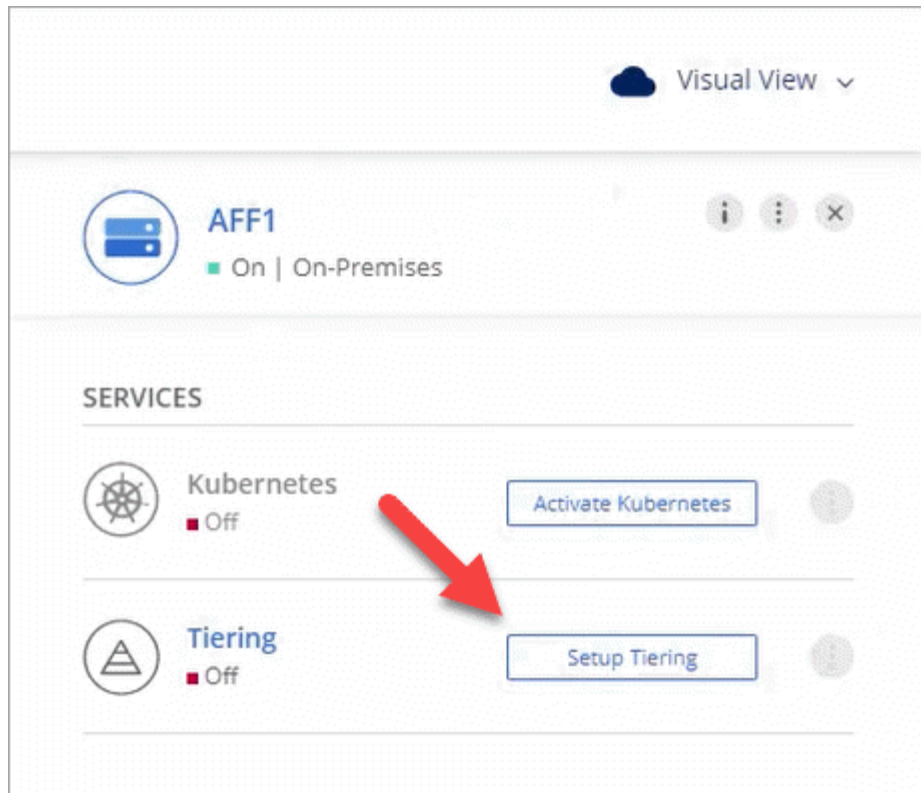
You're now on the Tiering dashboard.

3. Click **Set up Tiering** next to the cluster.

4. Complete the steps on the **Tiering Setup** page:

   a. **Bucket**: Add a new Google Cloud Storage bucket or select an existing bucket and click **Continue**.

   b. **Storage Class**: Select the storage class that you want to use for the tiered data and click **Continue**.

   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 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. Click **Continue** to select the volumes that you want to tier.

6. On the **Tier Volumes** page, set up tiering for each volume.

   Learn more about volume tiering policies.

   ◦ To select a tiering policy for just one volume, click the ✎ icon, select a tiering policy, and optionally adjust the cooling days.

◦ To select a tiering policy for several volumes, select multiple volumes, click **Modify selected volumes**, select a tiering policy, and optionally adjust the 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 from 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 data to StorageGRID. Data tiering is powered by NetApp's Cloud Tiering service.

Quick start

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

 Prepare to tier data to StorageGRID

You need the following:

- An AFF or FAS system with all-SSD aggregates that's running ONTAP 9.4 or later, and a connection over a user-specified port to StorageGRID.
- 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.
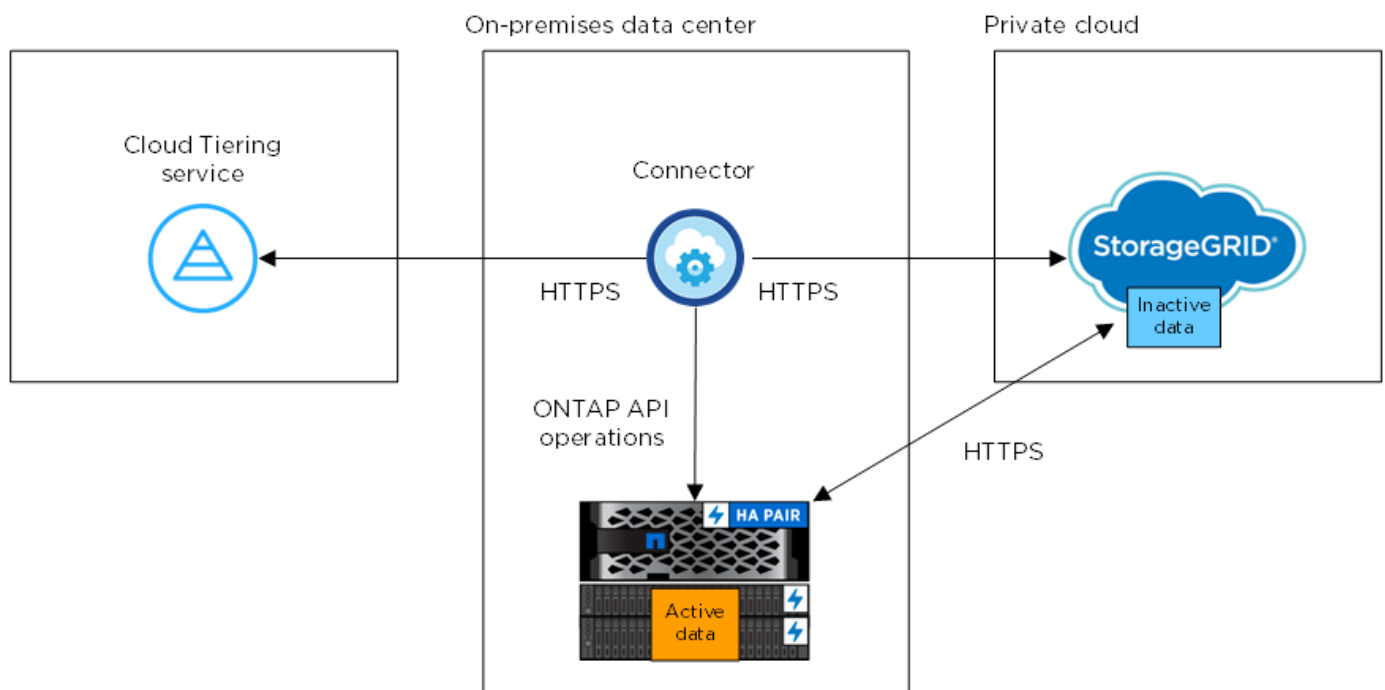
② Set up tiering

Select an on-prem working environment, click **Setup Tiering** 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:

> ℹ️ 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

Cloud Tiering supports AFF systems and all-SSD aggregates on FAS systems.

Supported ONTAP version

ONTAP 9.4 or later

Licensing

A FabricPool license isn't 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 tiered volumes. The LIF must be associated with the *IPspace* that ONTAP should use to connect to object storage.

  IPspaces enable network traffic segregation, allowing for separation of client traffic for privacy and security. Learn more about IPspaces.

  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.

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. For example, you can't tier data from SnapLock volumes or from MetroCluster configurations. Refer to ONTAP documentation for functionality or features not supported by FabricPool.

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

Preparing StorageGRID

StorageGRID must meet the following requirements.

Supported StorageGRID versions

StorageGRID 10.3 and later are 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
- Connector host requirements
- Installing the Connector on an existing 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 clusters

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.
- An AWS access key that has the required S3 permissions.

Steps

1. Select an on-prem cluster.
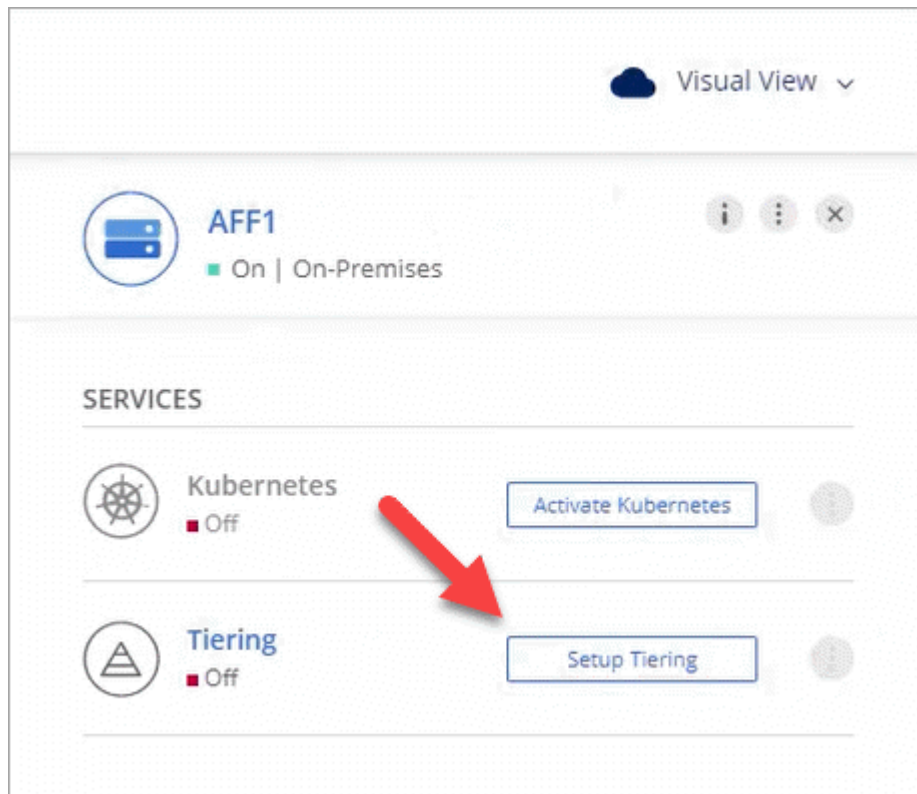
2. Click **Setup Tiering**.

You're now on the Tiering dashboard.

3. Click **Set up Tiering** next to the cluster.

4. Complete the steps on the **Tiering Setup** page:

   a. **Choose your provider**: Select StorageGRID.

   b. **Server**: Enter the FQDN of the StorageGRID server, enter the port that ONTAP should use for HTTPS communication with StorageGRID, and enter the access key and secret key for an AWS account that has the required S3 permissions.

   c. **Bucket**: Add a new bucket or select an existing bucket for the tiered data.

   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. Click **Continue** to select the volumes that you want to tier.

6. On the **Tier Volumes** page, set up tiering for each volume. Click the ✏ icon, select a tiering policy, optionally adjust the cooling days, and click **Apply**.

   Learn more about volume tiering policies.

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.

Set up licensing for Cloud Tiering

Pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license called *FabricPool*, or a combination of both. If you want to pay as you go, then you need to subscribe from the marketplace for the cloud provider to which you want to tier cold data. There's no need to subscribe from every marketplace.

A few notes before you read any further:

- If a FabricPool license is already installed on your cluster, then you're all set—there's nothing else that you need to do.

- If you've already subscribed to the Cloud Manager subscription in your cloud provider's marketplace, then you're automatically subscribed to Cloud Tiering, as well. You'll see an active subscription in the Cloud Tiering **Licensing** tab. You won't need to subscribe again.

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

Learn more about how licensing works for 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/occm/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/occm/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/occm/media/video_subscribing_gcp_tiering.mp4 *(video)*

Adding a tiering license to ONTAP

Bring your own license by purchasing an ONTAP FabricPool license from NetApp.

Steps

1. If you don't have a FabricPool license, [contact us to purchase one](#).

2. In Cloud Manager, click **Tiering** > **Licensing**.

3. In the Clusters List table, click **Activate license (BYOL)** for an on-prem ONTAP cluster.

4. Enter the serial number of the license and then enter the NetApp Support Site account that's associated with the serial number.

5. Click **Activate license**.

Result

Cloud Tiering registers the license and installs it on the cluster.

After you finish

If you purchase additional add-on capacity at a later time, the license on the cluster is automatically updated with the new capacity. There's no need to apply a new NetApp License File (NLF) to the cluster.

Managing data tiering from your clusters

Now that you've set up data tiering from your ONTAP clusters, you can tier data from additional volumes, change a volume's tiering policy, and more.

Tiering data from additional volumes

Set up data tiering for additional volumes at any time—for example, after creating a new volume.

Steps

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

2. From the **Cluster Dashboard**, click **Tier Volumes** for the cluster.

3. On the **Tier Volumes** page, set up tiering for each volume.

   [Learn more about volume tiering policies](#).

   > You don't need to configure the object storage because it was already configured when you initially set up tiering for the cluster. ONTAP will tier inactive data from these volumes to the same object store.

   ◦ To select a tiering policy for just one volume, click the ✎ icon, select a tiering policy, and optionally adjust the cooling days.

- To select a tiering policy for several volumes, select multiple volumes, click **Modify selected volumes**, select a tiering policy, and optionally adjust the cooling days.

Changing a volume's tiering policy

Changing the tiering policy for a volume changes how ONTAP tiers cold data to object storage. The change starts from the moment that you change the policy—it changes only the subsequent tiering behavior for the volume.

Steps

1. At the top of Cloud Manager, click **Tiering**.
2. From the **Cluster Dashboard**, click **Tier Volumes** for the cluster.
3. Click the ✏️ icon, select a tiering policy, optionally adjust the cooling days, and click **Apply**.

   [Learn more about volume tiering policies](#).

Managing tiering settings on aggregates

Each aggregate has two settings that you can adjust: the tiering fullness threshold and whether inactive data reporting is enabled.

Tiering fullness threshold

Setting the threshold to a lower number reduces the amount of data required to be stored on the performance tier before tiering takes place. This might be useful for large aggregates that contain little active data.

Setting the threshold to a higher number increases the amount of data required to be stored on the performance tier before tiering takes place. This might be useful for solutions designed to tier only

when aggregates are near maximum capacity.

Inactive data reporting

Inactive data reporting (IDR) uses a 31-day cooling period to determine which data is considered inactive. The amount of cold data that is tiered is dependent on the tiering policies set on volumes. This amount might be different than the amount of cold data detected by IDR using a 31-day cooling period.

> 💡 It's best to keep IDR enabled because it helps to identify your inactive data and savings opportunities. IDR must remain enabled if data tiering was enabled on an aggregate.

Steps

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

2. From the **Cloud Tiering** page, click the menu icon for a cluster and select **Manage Aggregates**.
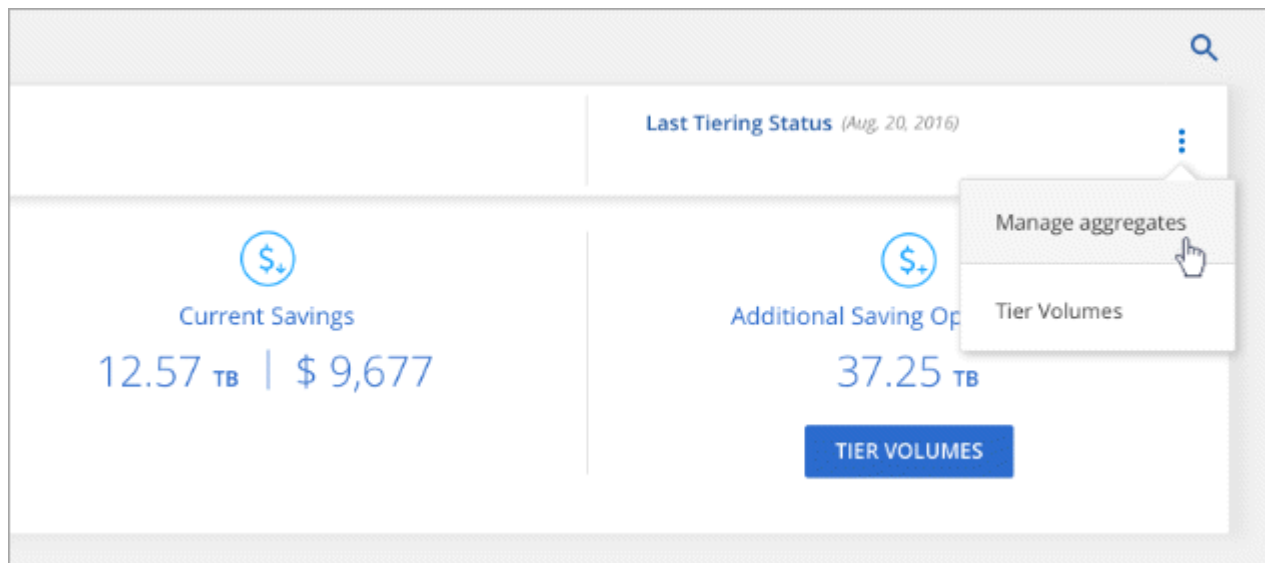
3. On the **Manage Aggregates** page, click the ✏️ icon for an aggregate in the table.

4. Modify the fullness threshold and choose whether to enable or disable inactive data reporting.
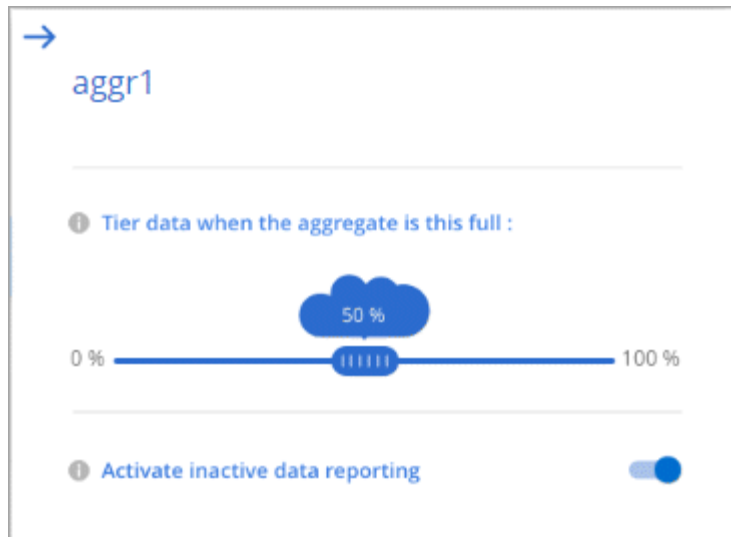
5. Click **Apply**.

Reviewing tiering info for a cluster

You might want to see how much data is in the cloud tier and how much data is on disks. Or, you might want to see the amount of hot and cold data on the cluster's disks. Cloud Tiering provides this information for each cluster.
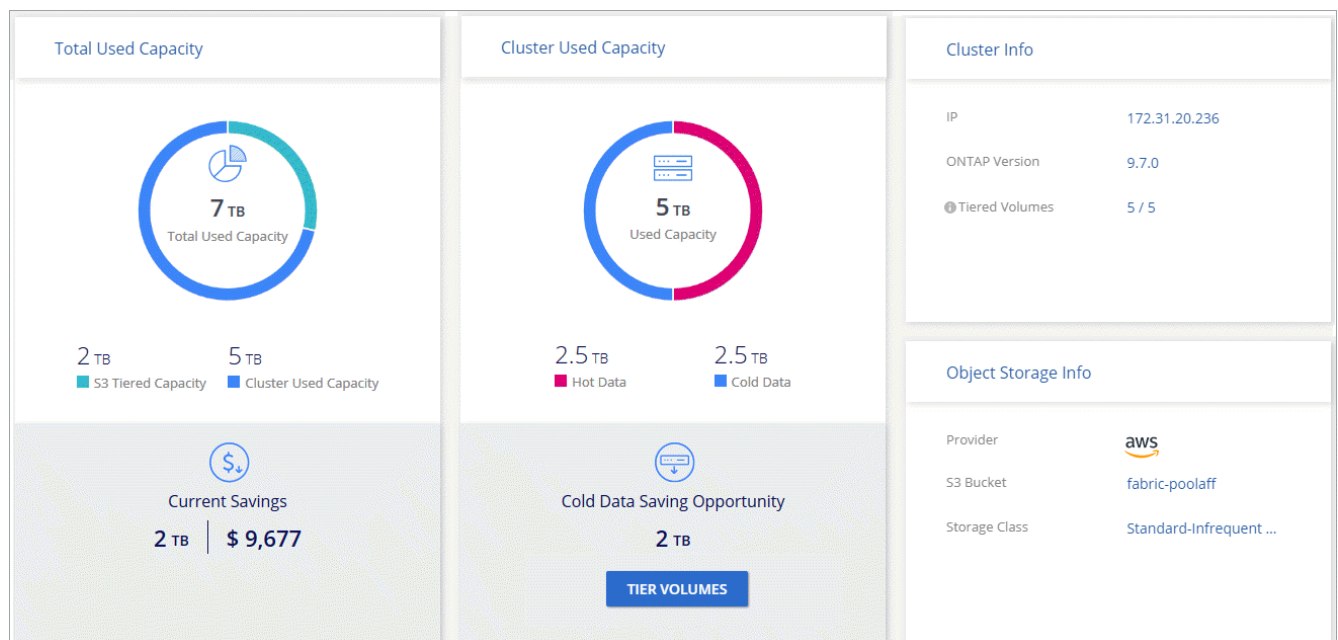
Steps

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

2. From the **Cluster Dashboard**, click **More info** for a cluster.
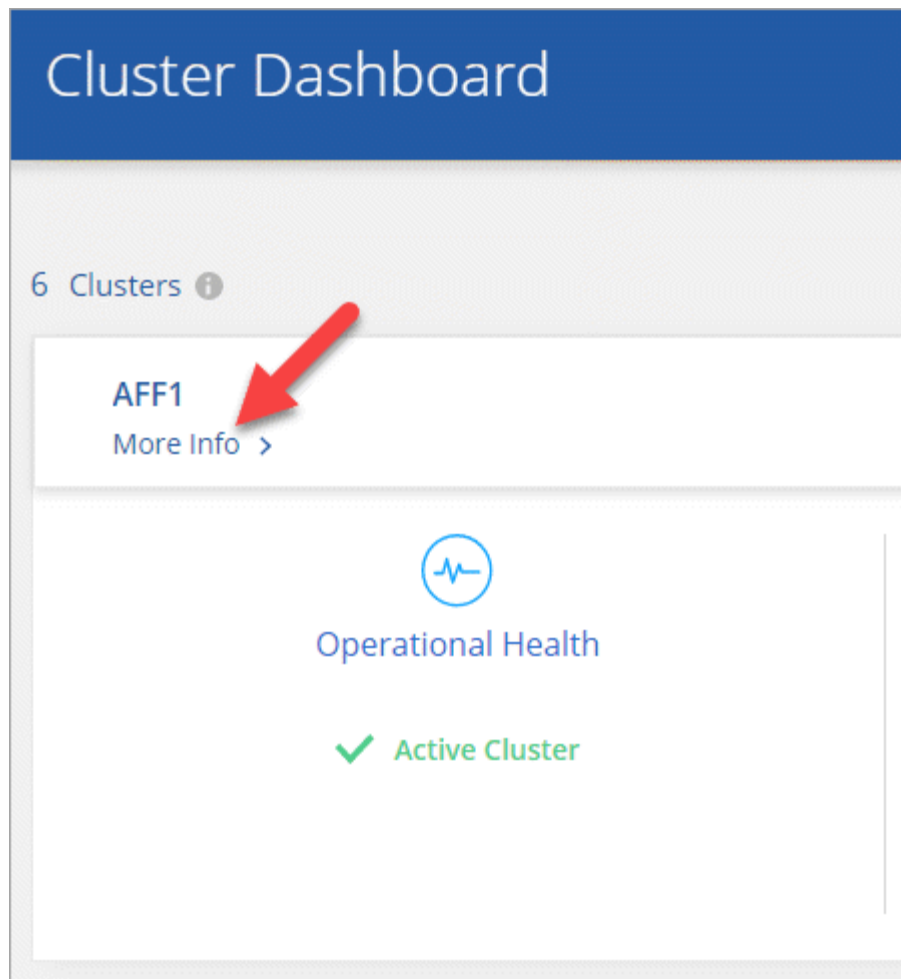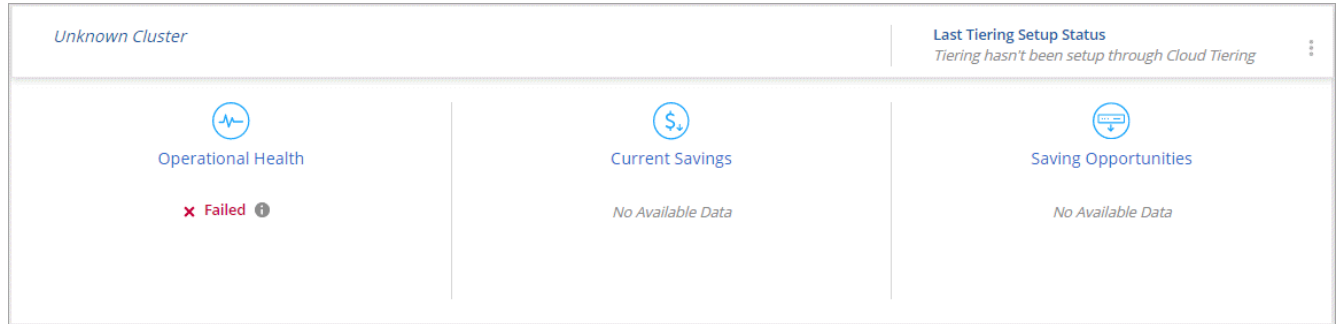
3. Review details about the cluster.

   Here's an example:

Fixing operational health

Failures can happen. When they do, Cloud Tiering displays a "Failed" operational health status on the Cluster Dashboard. The health reflects the status of the ONTAP system and Cloud Manager.

Steps

1. Identify any clusters that have an operational health of "Failed."

2. Hover over the ⓘ icon to see the failure reason.

3. Correct the issue:

   a. Verify that the ONTAP cluster is operational and that it has an inbound and outbound connection to your object storage provider.

   b. Verify that Cloud Manager has outbound connections to the Cloud Tiering service, to the object store, and to the ONTAP clusters that it discovers.

Get an overview of data tiering from your clusters

Cloud Tiering provides an aggregated view of data tiering from each of your on-premises clusters. This overview provides a clear picture of your environment and enables you to take proper actions.

Cloud Tiering provides the following details about your environment:
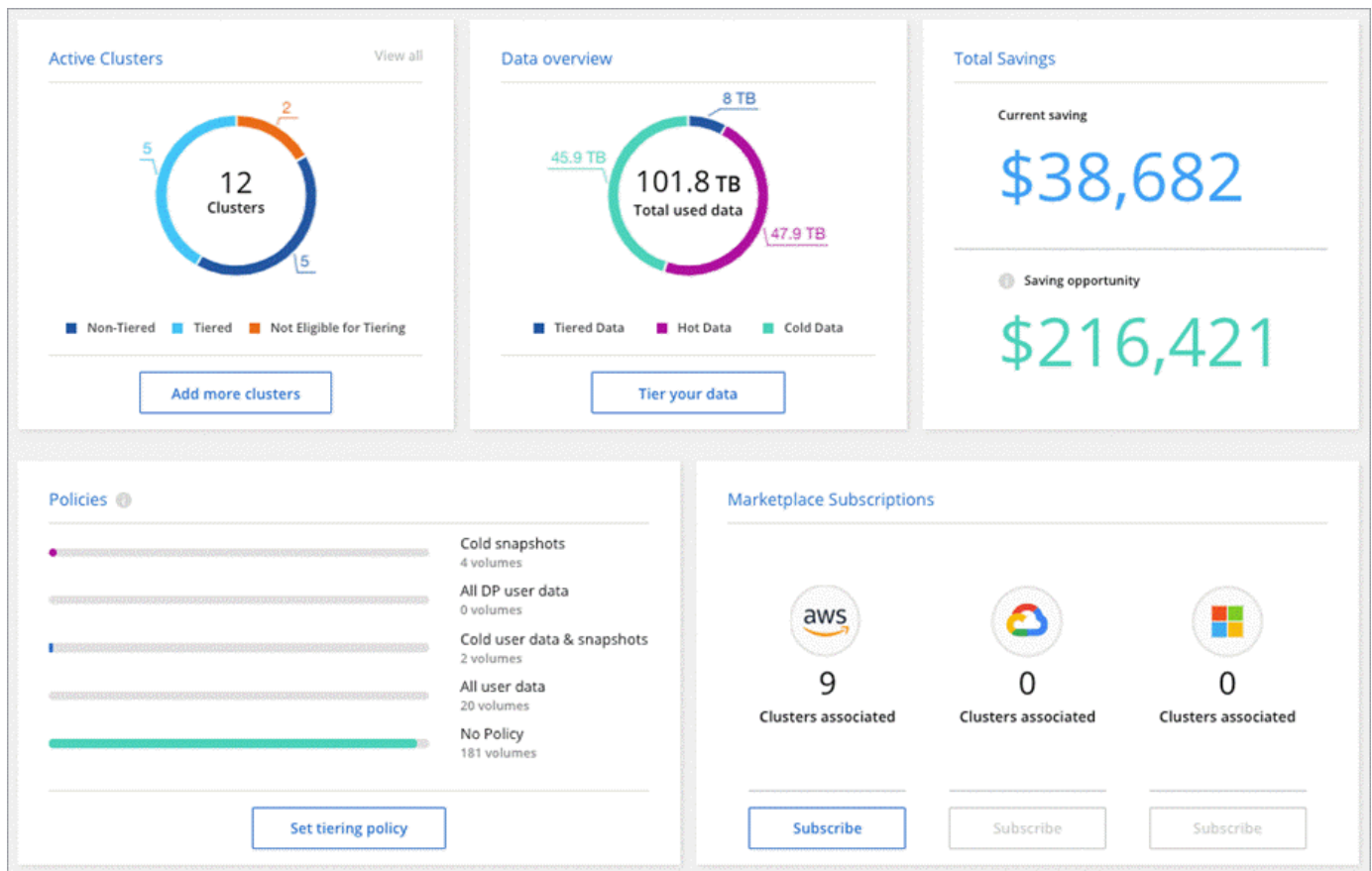
Active Clusters

The number of clusters that are currently tiering data to the cloud, the clusters that aren't tiering data to the cloud, and the number of clusters that don't support data tiering.

Data Overview

The amount of data that was tiered to the cloud, and the amount of hot and cold data on the cluster.

Total Savings

The amount of money that you've saved by tiering data to the cloud, as well as the amount of money that you could save by tiering more data to the cloud.

Policies

The number of times that each tiering policy has been applied to a volume.

Marketplace Subscriptions

The number of clusters associated with each type of Marketplace Subscription and an indication about your subscription status.

Steps

1. Click **Tiering** > **On-Prem Overview**.

Cloud Tiering technical FAQ

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

ONTAP

The following questions relate to ONTAP.

What are the requirements for my ONTAP cluster?

It depends on where you tier the cold data. Refer to the following:

- Tiering data from on-premises ONTAP clusters to Amazon S3
- Tiering data from on-premises ONTAP clusters to Azure Blob storage
- Tiering data from on-premises ONTAP clusters to Google Cloud Storage
- Tiering data from on-premises ONTAP clusters to StorageGRID

Does Cloud Tiering enable inactive data reporting?

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

> ℹ️ Cloud Tiering enables inactive data reporting on HDD aggregates if the cluster is running ONTAP 9.6 or later.

Can I tier data from NAS volumes and SAN volumes?

You can use Cloud Tiering to tier data from NAS volumes to the public cloud and from SAN volumes to a private cloud using StorageGRID.

What about Cloud Volumes ONTAP?

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.

From the Cluster Dashboard, you can view tiering information similar to an on-prem ONTAP cluster: operational health, current savings, savings opportunities, details about volumes and aggregates, and more.

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'll still set up tiering the same way: from the working environment in Cloud Manager.

Object storage

The following questions relate to object storage.

Which object storage providers are supported?

Amazon S3, Azure Blob storage, Google Cloud Storage, and StorageGRID using the S3 protocol are supported.

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-IA*, or *Intelligent* storage class. See Supported S3 storage classes for more details.

Which Azure Blob access tiers are supported?

Cloud Tiering automatically uses the *Hot* access tier for your inactive data.

Which storage classes are supported for Google Cloud Storage?

Cloud Tiering uses the *Standard* storage class for inactive data.

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

One object store for the entire cluster.

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

No, Cloud Tiering does not support object lifecycle management rules that move or delete data from object stores.

Connectors

The following questions relate to Connectors.

Where does the Connector need to be installed?

- When tiering data to S3, a Connector can reside in an AWS VPC or on your premises.

- When tiering data to Blob storage, a Connector must reside in an Azure VNet.

- When tiering data to Google Cloud Storage, a Connector must reside in a Google Cloud Platform VPC.

- When tiering data to StorageGRID, a Connector must reside on an on premises Linux host.

Networking

The following questions relate to networking.

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 from on-premises ONTAP clusters to Amazon S3
- Tiering data from on-premises ONTAP clusters to Azure Blob storage
- Tiering data from on-premises ONTAP clusters to Google Cloud Storage
- Tiering data from on-premises ONTAP clusters to StorageGRID

Permissions

The following questions relate to permissions.

What permissions are required in AWS?

Permissions are required to manage the S3 bucket.

What permissions are required in Azure?

No extra permissions are needed outside of the permissions that you need to provide to Cloud Manager.

What permissions are required in Google Cloud Platform?

Storage Admin permissions are needed for a service account that has storage access keys.

What permissions are required for StorageGRID?

S3 permissions are needed.

Reference

Supported S3 storage classes and regions

Cloud Tiering supports several S3 storage classes and most regions.

Supported S3 storage classes

Cloud Tiering can apply a lifecycle rule so the data transitions from the *Standard* storage class to another storage class after 30 days. You can choose from the following storage classes:

- Standard-Infrequent Access
- One Zone-IA
- Intelligent

If you choose Standard, then the data remains in that storage class.

Learn about S3 storage classes.

Supported AWS regions

Cloud Tiering supports the following AWS regions.

Asia Pacific

- Mumbai
- Seoul
- Singapore
- Sydney
- Tokyo

Europe

- Frankfurt
- Ireland
- London

- Paris

- Stockholm

North America

- Canada Central

- GovCloud (US-West) – starting with ONTAP 9.3

- US East (N. Virginia)

- US East (Ohio)

- US West (N. California)

- US West (Oregon)

South America

- São Paulo

Supported Azure Blob access tiers and regions

Cloud Tiering supports the *Hot* access tier and most regions.

Supported Azure Blob access tiers

When you set up data tiering to Azure, Cloud Tiering automatically uses the *Hot* access tier for your inactive data.

Supported Azure regions

Cloud Tiering supports the following Azure regions.

Africa

- South Africa North

Asia Pacific

- Australia East

- Australia Southeast

- East Asia

- Japan East

- Japan West

- Korea Central

- Korea South

- Southeast Asia

Europe

- France Central
- Germany Central
- Germany Northeast
- North Europe
- UK South
- UK West
- West Europe

North America

- Canada Central
- Canada East
- Central US
- East US
- East US 2
- North Central US
- South Central US
- West US
- West US 2
- West Central US

South America

- Brazil South

Supported Google Cloud storage classes and regions

Cloud Tiering supports the Standard storage class and most Google Cloud regions.

Supported access tiers

Cloud Tiering uses the *Standard* access tier for your inactive data.

Supported Google Cloud regions

Cloud Tiering supports the following regions.

Americas

- Iowa
- Los Angeles
- Montreal
- N. Virginia
- Oregon
- Sao-Paulo
- South Carolina

Asia Pacific

- Hong Kong
- Mumbai
- Osaka
- Singapore
- Sydney
- Taiwan
- Tokyo

Europe

- Belgium
- Finland
- Frankfurt
- London
- Netherlands
- Zurich