



Get started

Cloud Manager

NetApp
December 07, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_tiering_onprem_aws.html on December 07, 2020. Always check docs.netapp.com for the latest.

Table of Contents

- Get started..... 1
 - Tiering data from on-premises ONTAP clusters to Amazon S3..... 1
 - Tiering data from on-premises ONTAP clusters to Azure Blob storage..... 7
 - Tiering data from on-premises ONTAP clusters to Google Cloud Storage 12
 - Tiering data from on-premises ONTAP clusters to StorageGRID 17

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.



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.



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.



Set up licensing

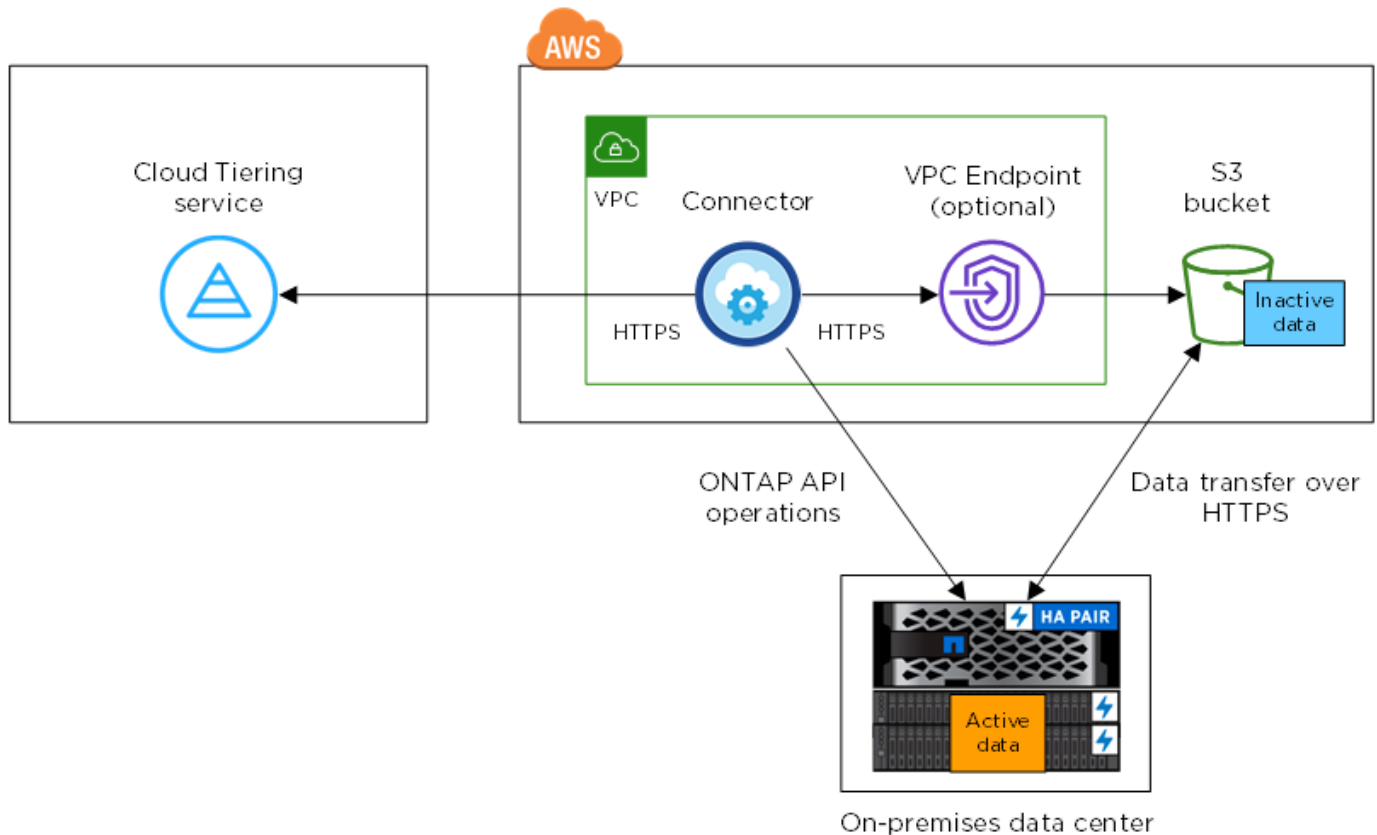
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both:

- 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

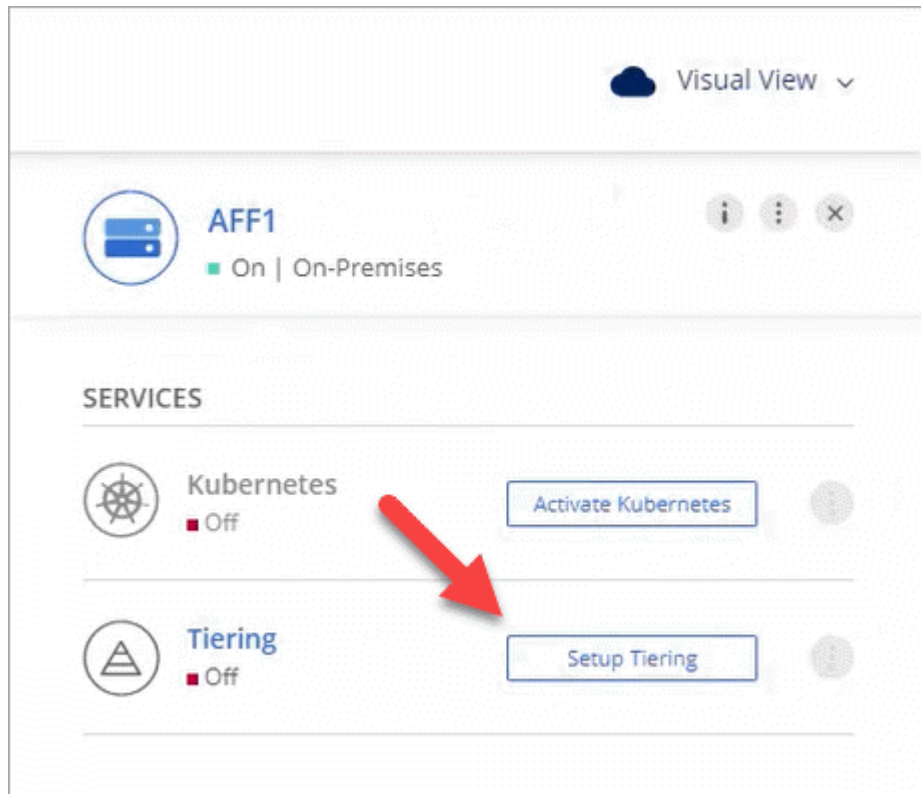
After you prepare your AWS environment, start tiering inactive data from your first cluster.

What you'll need

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

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. **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**.

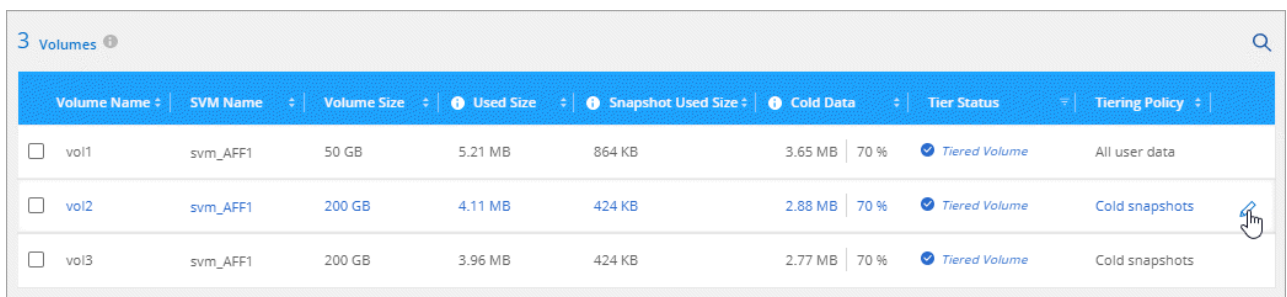
Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your cloud provider's object storage.

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

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

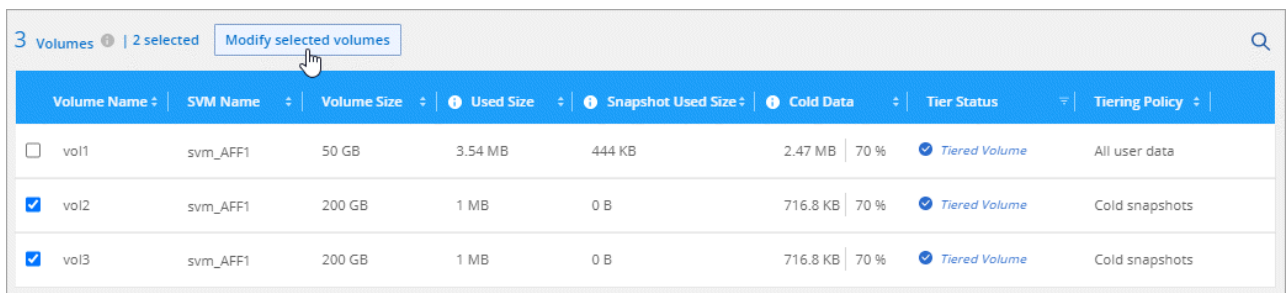
[Learn more about volume tiering policies.](#)

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



Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy
<input type="checkbox"/> vol1	svm_AFF1	50 GB	5.21 MB	864 KB	3.65 MB 70 %	Tiered Volume	All user data
<input type="checkbox"/> vol2	svm_AFF1	200 GB	4.11 MB	424 KB	2.88 MB 70 %	Tiered Volume	Cold snapshots
<input type="checkbox"/> vol3	svm_AFF1	200 GB	3.96 MB	424 KB	2.77 MB 70 %	Tiered Volume	Cold snapshots

- 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.



Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy
<input type="checkbox"/> vol1	svm_AFF1	50 GB	3.54 MB	444 KB	2.47 MB 70 %	Tiered Volume	All user data
<input checked="" type="checkbox"/> vol2	svm_AFF1	200 GB	1 MB	0 B	716.8 KB 70 %	Tiered Volume	Cold snapshots
<input checked="" type="checkbox"/> vol3	svm_AFF1	200 GB	1 MB	0 B	716.8 KB 70 %	Tiered Volume	Cold snapshots

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.



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.



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.



Set up licensing

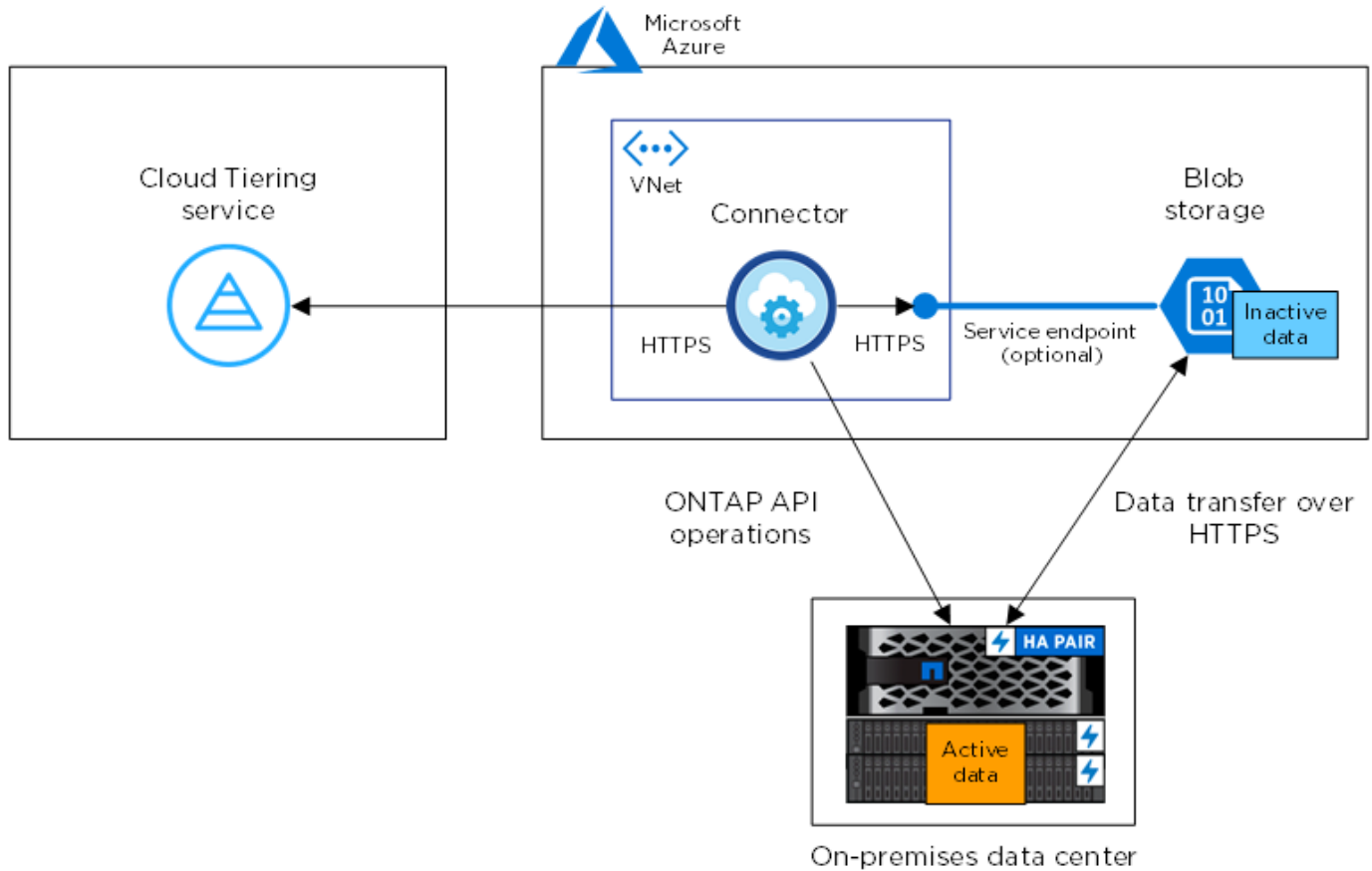
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both:

- 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:



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

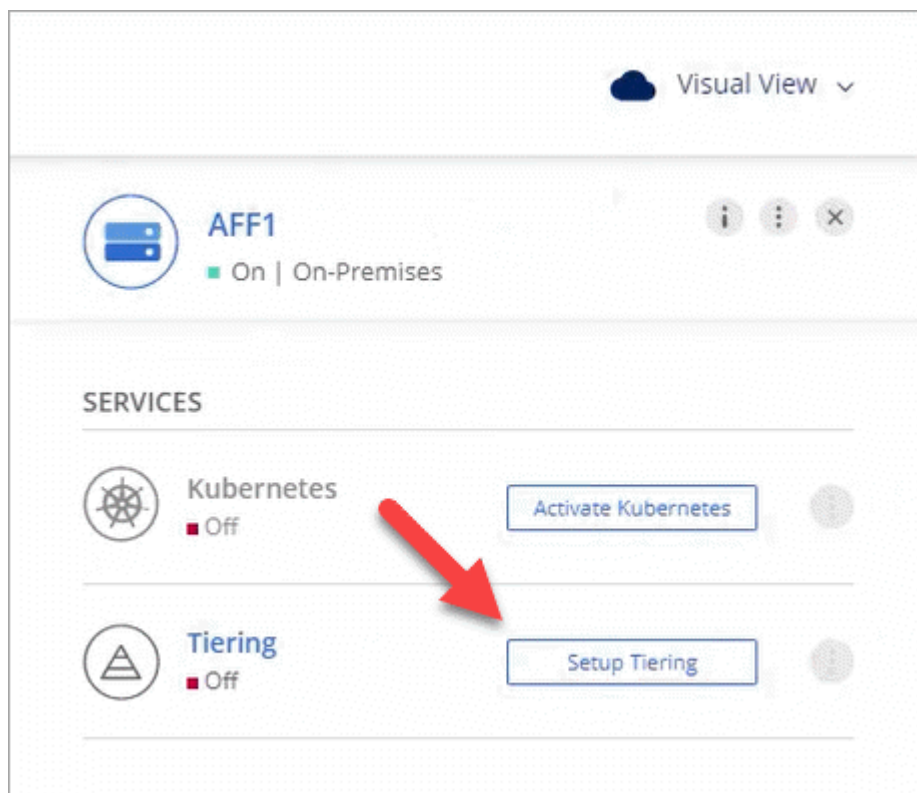
After you prepare your Azure environment, start tiering inactive data from your first cluster.

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.

3 Volumes ⓘ									
	Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data		Tier Status	Tiering Policy
<input type="checkbox"/>	vol1	svm_AFF1	50 GB	5.21 MB	864 KB	3.65 MB 70 %		Tiered Volume	All user data
<input type="checkbox"/>	vol2	svm_AFF1	200 GB	4.11 MB	424 KB	2.88 MB 70 %		Tiered Volume	Cold snapshots 
<input type="checkbox"/>	vol3	svm_AFF1	200 GB	3.96 MB	424 KB	2.77 MB 70 %		Tiered Volume	Cold snapshots

- 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.

3 Volumes ⓘ 2 selected Modify selected volumes									
	Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data		Tier Status	Tiering Policy
<input type="checkbox"/>	vol1	svm_AFF1	50 GB	3.54 MB	444 KB	2.47 MB 70 %		Tiered Volume	All user data
<input checked="" type="checkbox"/>	vol2	svm_AFF1	200 GB	1 MB	0 B	716.8 KB 70 %		Tiered Volume	Cold snapshots
<input checked="" type="checkbox"/>	vol3	svm_AFF1	200 GB	1 MB	0 B	716.8 KB 70 %		Tiered Volume	Cold snapshots

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.



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.



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.



Set up licensing

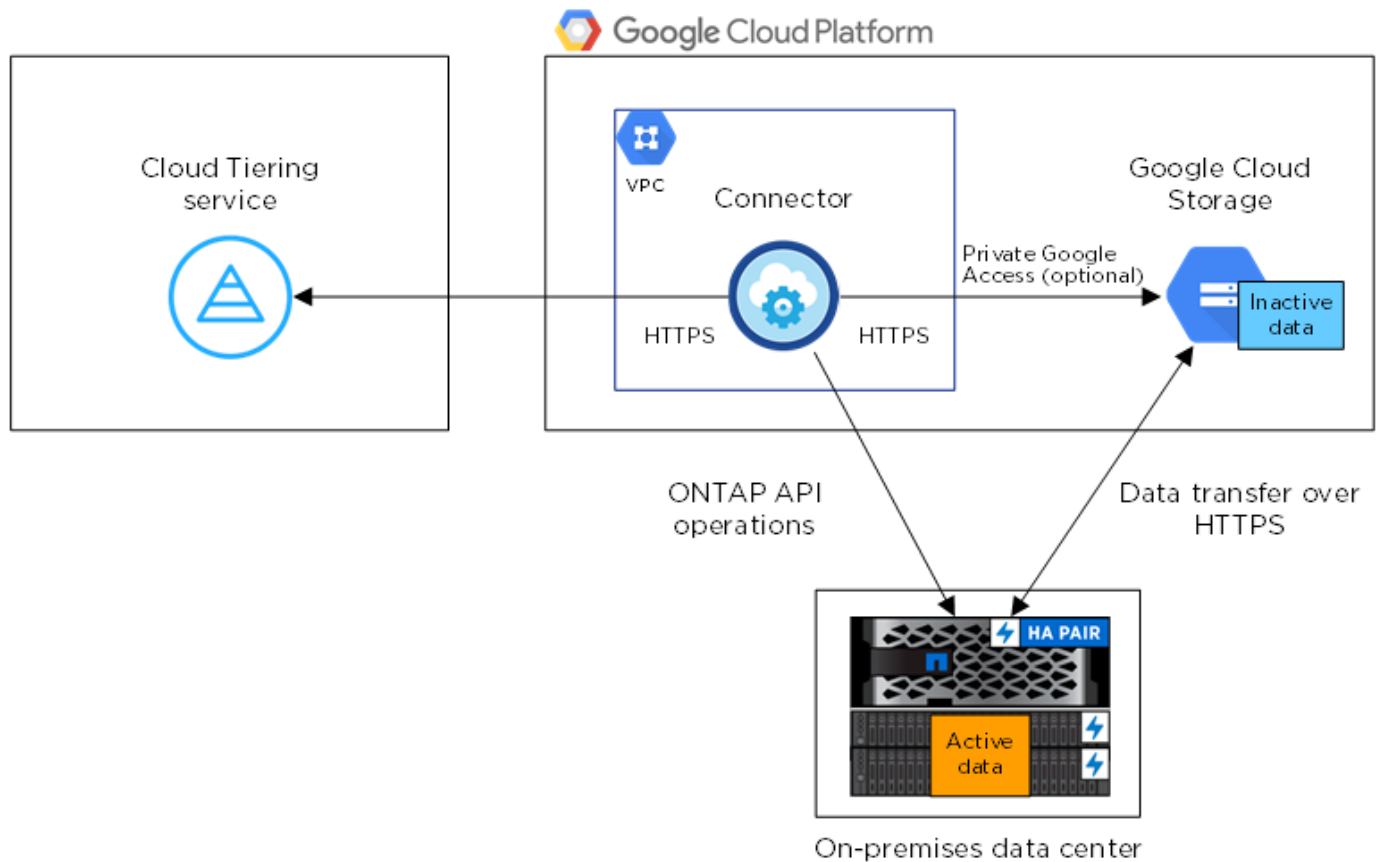
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both:

- 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](#)

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

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](#).



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

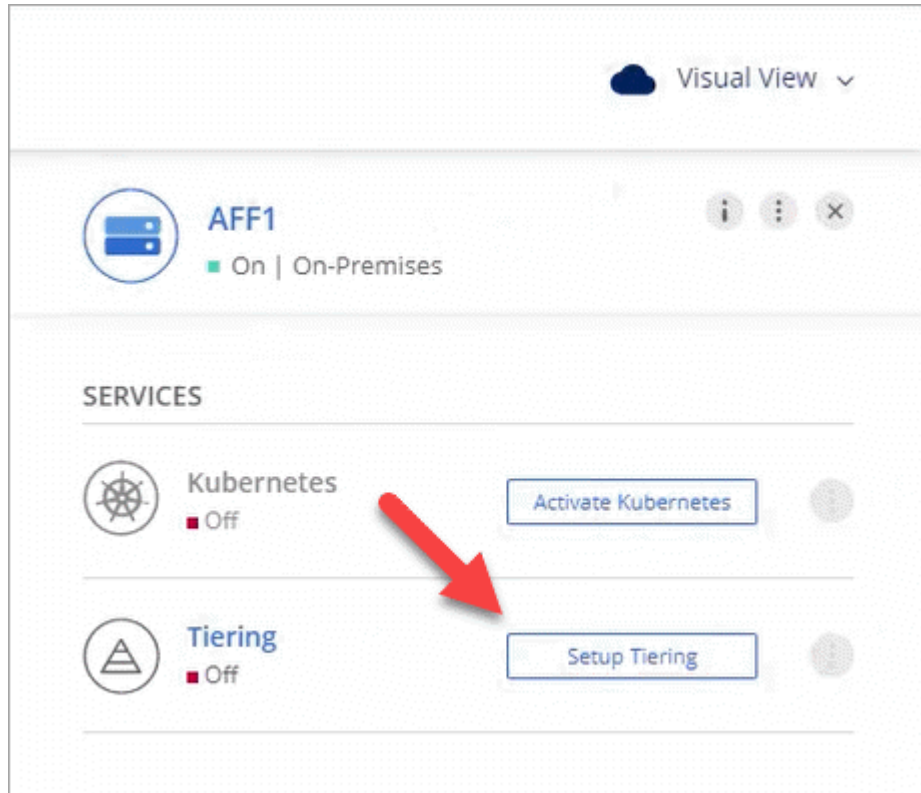
After you prepare your Google Cloud environment, start tiering inactive data from your first cluster.

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.

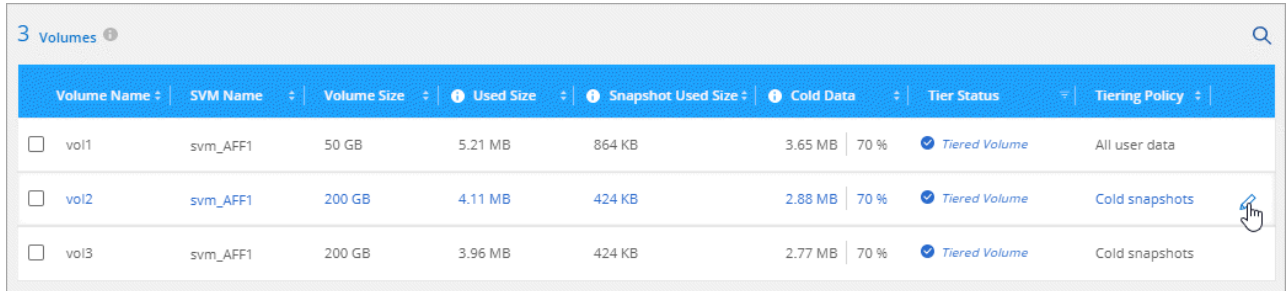
3. Click **Set up Tiering** next to the cluster.
4. Complete the steps on the **Tiering Setup** page:
 - a. **Bucket:** Add a new Google Cloud Storage bucket or select an existing bucket and click **Continue**.
 - b. **Storage Class:** Select the storage class that you want to use for the tiered data 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.

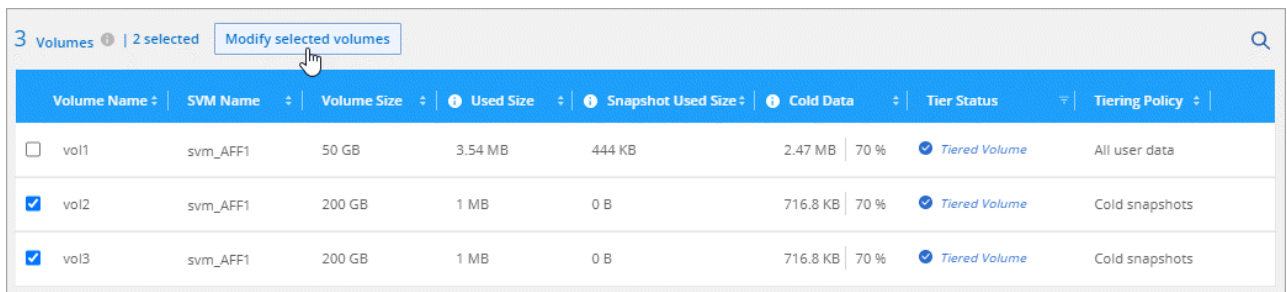
[Learn more about volume tiering policies.](#)

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



Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy
<input type="checkbox"/> vol1	svm_AFF1	50 GB	5.21 MB	864 KB	3.65 MB 70 %	Tiered Volume	All user data
<input type="checkbox"/> vol2	svm_AFF1	200 GB	4.11 MB	424 KB	2.88 MB 70 %	Tiered Volume	Cold snapshots 
<input type="checkbox"/> vol3	svm_AFF1	200 GB	3.96 MB	424 KB	2.77 MB 70 %	Tiered Volume	Cold snapshots

- 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.



Volume Name	SVM Name	Volume Size	Used Size	Snapshot Used Size	Cold Data	Tier Status	Tiering Policy
<input type="checkbox"/> vol1	svm_AFF1	50 GB	3.54 MB	444 KB	2.47 MB 70 %	Tiered Volume	All user data
<input checked="" type="checkbox"/> vol2	svm_AFF1	200 GB	1 MB	0 B	716.8 KB 70 %	Tiered Volume	Cold snapshots
<input checked="" type="checkbox"/> vol3	svm_AFF1	200 GB	1 MB	0 B	716.8 KB 70 %	Tiered Volume	Cold snapshots

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.

1

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

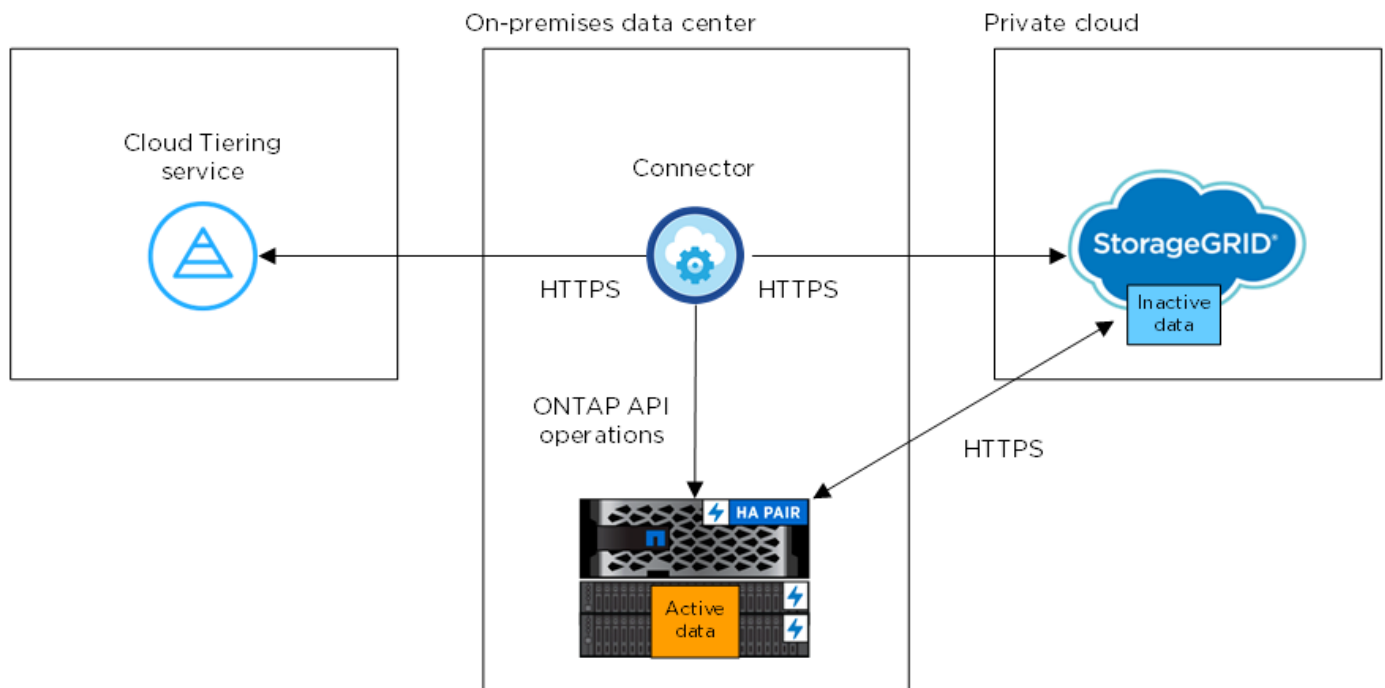
Set up tiering

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:



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](#).



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

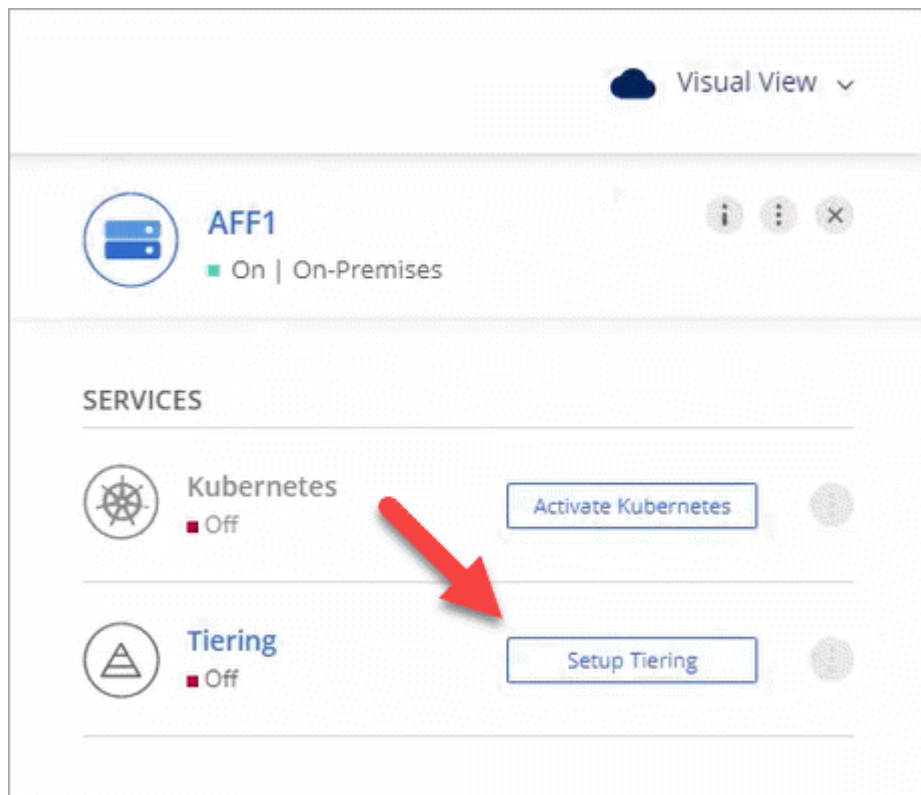
After you prepare your environment, start tiering inactive data from your first cluster.

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.](#)

Tier Volumes

Tier volumes

Learn how much you can save with each Tiering Policy

50 Volumes

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.](#)

Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.