



Tier on-prem data to the cloud

Cloud Tiering

NetApp
July 12, 2022

This PDF was generated from <https://docs.netapp.com/us-en/cloud-manager-tiering/task-tiering-onprem-aws.html> on July 12, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- Tier on-prem data to the cloud 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 13
 - Tiering data from on-premises ONTAP clusters to StorageGRID 19
 - Tiering data from on-premises ONTAP clusters to S3 object storage 24

Tier on-prem data to the cloud

Tiering data from on-premises ONTAP clusters to Amazon S3

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

Quick start

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

1

Prepare to tier data to Amazon S3

You need the following:

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

2

Set up tiering

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

3

Set up licensing

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

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

Requirements

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

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



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

Preparing your ONTAP clusters

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

Supported ONTAP platforms

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

Supported ONTAP version

ONTAP 9.2 or later

Cluster networking requirements

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

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

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

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

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

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

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

Supported volumes and aggregates

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



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

Discovering an ONTAP cluster

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

[Learn how to discover a cluster.](#)

Creating or switching Connectors

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

- [Learn about Connectors](#)
- [Creating a Connector in AWS](#)
- [Installing the Connector on a Linux host](#)
- [Switching between Connectors](#)

Preparing networking for the Connector

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

Steps

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

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

Preparing Amazon S3

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

The S3 bucket must be in a [region that supports Cloud Tiering](#).



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

Steps

1. Provide the following permissions to the IAM user:

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

[AWS Documentation: Creating a Role to Delegate Permissions to an IAM User](#)

2. Create or locate an access key.

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

[AWS Documentation: Managing Access Keys for IAM Users](#)

Tiering inactive data from your first cluster to Amazon S3

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

What you'll need

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

Steps

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



3. **Choose your provider:** This page appears only when using an on-prem Connector. Select **Amazon Web Services** and click **Continue**.

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

- a. **S3 Bucket:** Add a new S3 bucket or select an existing S3 bucket that starts with the prefix *fabric-pool* and click **Continue**.

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

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

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

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

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



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

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

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

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

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

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

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

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

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



Result

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

What's next?

Be sure to [subscribe to the Cloud Tiering service](#).

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

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

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

Quick start

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

1

Prepare to tier data to Azure Blob storage

You need the following:

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

2

Set up tiering

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

3

Set up licensing

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

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

Requirements

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

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



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

Preparing your ONTAP clusters

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

Supported ONTAP platforms

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

Supported ONTAP version

ONTAP 9.4 or later

Cluster networking requirements

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

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

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

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

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

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

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

Supported volumes and aggregates

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



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

Discovering an ONTAP cluster

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

[Learn how to discover a cluster.](#)

Creating or switching Connectors

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

- [Learn about Connectors](#)

- [Creating a Connector in Azure](#)
- [Installing the Connector on a Linux host](#)
- [Switching between Connectors](#)

Verify that you have the necessary Connector permissions

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

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

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

Preparing networking for the Connector

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

Steps

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

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

Preparing Azure Blob storage

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

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

The Blob container must be in a [region that supports Cloud Tiering](#).



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

Tiering inactive data from your first cluster to Azure Blob storage

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

What you'll need

An on-premises working environment.

Steps

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



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

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

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

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

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

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


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

[Verify that you have the necessary Connector permissions](#) for the life cycle management feature.

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

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

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

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

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

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



Result

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

What's next?

Be sure to [subscribe to the Cloud Tiering service](#).

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

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

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

Quick start

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

1

Prepare to tier data to Google Cloud Storage

You need the following:

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

2

Set up tiering

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

3

Set up licensing

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

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

Requirements

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

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



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

Preparing your ONTAP clusters

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

Supported ONTAP platforms

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

Supported ONTAP versions

ONTAP 9.6 or later

Cluster networking requirements

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

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

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

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

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

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

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

Supported volumes and aggregates

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



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

Discovering an ONTAP cluster

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

[Learn how to discover a cluster.](#)

Creating or switching Connectors

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

- [Learn about Connectors](#)
- [Creating a Connector in GCP](#)
- [Switching between Connectors](#)

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

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

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

Preparing Google Cloud Storage

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

The Cloud Storage buckets must be in a [region that supports Cloud Tiering](#).



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

Steps

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

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

Tiering inactive data from your first cluster to Google Cloud Storage

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

What you'll need

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

Steps

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



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

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

If you choose **Keep data in this storage class**, then the data remains in the that storage class. [See supported storage classes](#).

Storage Class Life Cycle Management

We'll move the tiered data through the storage classes that you include in the life cycle. [Learn more about Google Cloud Storage classes.](#)

STORAGE CLASS SETUP ⓘ

Standard

☒ Move data from Standard to Nearline after days

☐ Keep data in this storage class

↓

Nearline

☒ Move data from Nearline to Coldline after days

☐ Keep data in this storage class

↓

Coldline

☐ Move data from Coldline to Archive after days

☒ Keep data in this storage class

↓

Archive

No Time Limit

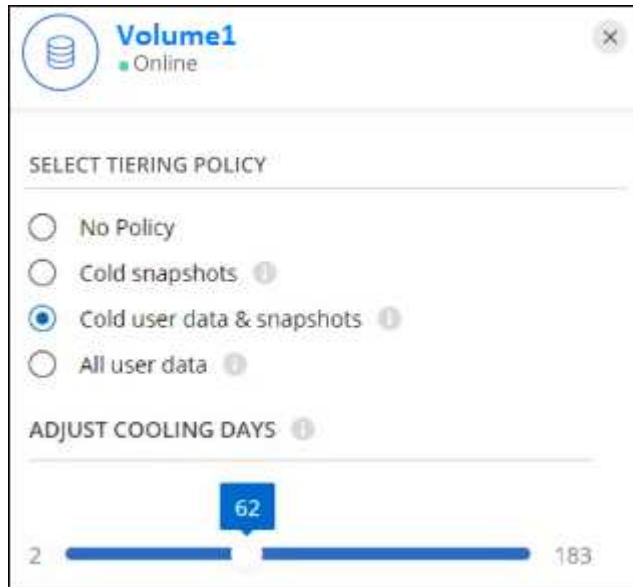
Note that the life cycle rule is applied to all objects in the selected bucket.

- c. **Credentials:** Enter the storage access key and secret key for a service account that has the Storage Admin role.
- d. **Cluster Network:** Select the IPspace that ONTAP should use to connect to object storage.

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

4. Click **Continue** to select the volumes that you want to tier.
5. On the *Tier Volumes* page, select the volumes that you want to configure tiering for and launch the Tiering Policy page:
 - To select all volumes, check the box in the title row (☒ Volume Name) and click **Configure volumes**.
 - To select multiple volumes, check the box for each volume (☒ Volume_1) and click **Configure volumes**.
 - To select a single volume, click the row (or  icon) for the volume.
6. In the *Tiering Policy* dialog, select a tiering policy, optionally adjust the cooling days for the selected volumes, and click **Apply**.

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



Result

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

What's next?

[Be sure to subscribe to the Cloud Tiering service.](#)

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

Tiering data from on-premises ONTAP clusters to StorageGRID

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

Quick start

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

1

Prepare to tier data to StorageGRID

You need the following:

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

2

Set up tiering

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

Requirements

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

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



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

Preparing your ONTAP clusters

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

Supported ONTAP platforms

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

Supported ONTAP version

ONTAP 9.4 or later

Licensing

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

Cluster networking requirements

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

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

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

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

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

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

Supported volumes and aggregates

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



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

Discovering an ONTAP cluster

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

[Learn how to discover a cluster.](#)

Preparing StorageGRID

StorageGRID must meet the following requirements.

Supported StorageGRID versions

StorageGRID 10.3 and later is supported.

S3 credentials

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

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

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

Object versioning

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

Creating or switching Connectors

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

- [Learn about Connectors](#)
- [Installing the Connector on a Linux host](#)
- [Switching between Connectors](#)

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

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

Tiering inactive data from your first cluster to StorageGRID

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

What you'll need

- [An on-premises working environment.](#)
- The FQDN of the StorageGRID Gateway Node, and the port that will be used for HTTPS communications.
- An AWS access key that has the required S3 permissions.

Steps

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




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

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

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

Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to StorageGRID object storage.

5. On the *Tier Volumes* page, select the volumes that you want to configure tiering for and launch the Tiering Policy page:
 - To select all volumes, check the box in the title row (☒ Volume Name) and click **Configure volumes**.
 - To select multiple volumes, check the box for each volume (☒ Volume_1) and click **Configure volumes**.
 - To select a single volume, click the row (or  icon) for the volume.
6. In the *Tiering Policy* dialog, select a tiering policy, optionally adjust the cooling days for the selected volumes, and click **Apply**.

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



Result

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

What's next?

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

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

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

Customers who want to use object stores that are not officially supported as a cloud tier can do so using these instructions. Customers must test and confirm that the object store meets their requirements.



NetApp does not support nor is liable for any issues arising from any third-party Object Store Service, specifically where it does not have agreed support arrangements with the third party with whom the product originated. It is acknowledged and agreed that NetApp shall not be liable for any associated damage or otherwise be required to provide support on that third-party product.

Quick start

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

1

Prepare to tier data to S3-compatible object storage

You need the following:

- An on-prem ONTAP cluster that's running ONTAP 9.8 or later, and a connection over a user-specified port

to the S3-compatible object storage. [Learn how to discover a cluster.](#)

- The FQDN, Access Key, and Secret Key for the object storage server so that the ONTAP cluster can access the bucket.
- A Connector installed on your premises.
- Networking for the Connector that enables an outbound HTTPS connection to the ONTAP cluster, to the S3-compatible object storage, and to the Cloud Tiering service.

2

Set up tiering

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

3

Set up licensing

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

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

Requirements

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

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





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

Preparing your ONTAP clusters

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

Supported ONTAP platforms

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

Supported ONTAP version

ONTAP 9.8 or later

Cluster networking requirements

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

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

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

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

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

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

Supported volumes and aggregates

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



Cloud Tiering supports both FlexVol and FlexGroup volumes.

Discovering an ONTAP cluster

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

[Learn how to discover a cluster.](#)

Preparing S3-compatible object storage

S3-compatible object storage must meet the following requirements.

S3 credentials

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

Cloud Tiering uses the keys to access your bucket.

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

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

Creating or switching Connectors

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

- [Learn about Connectors](#)
- [Installing the Connector on a Linux host](#)
- [Switching between Connectors](#)

Preparing networking for the Connector

Ensure that the Connector has the required networking connections.

Steps

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

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

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

What you'll need

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

Steps

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



3. **Choose your provider:** Select **S3 Compatible** and click **Continue**.

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

- Server:** Enter the FQDN of the S3-compatible object storage server, the port that ONTAP should use for HTTPS communication with the server, and the access key and secret key for an account that has the required S3 permissions.
- Bucket:** Add a new bucket or select an existing bucket and click **Continue**.
- Cluster Network:** Select the IPspace that ONTAP should use to connect to object storage and click **Continue**.

Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your S3-compatible object storage.

5. On the *Success* page click **Continue** to set up your volumes now.

6. On the *Tier Volumes* page, select the volumes that you want to configure tiering for and click **Continue**:

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



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

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



Result

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

What's next?

[Be sure to subscribe to the Cloud Tiering service.](#)

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

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

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

Trademark Information

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