



Manage ONTAP clusters

Cloud Manager

NetApp

June 15, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_discovering_ontap.html on June 15, 2020.
Always check docs.netapp.com for the latest.

Table of Contents

- Manage ONTAP clusters 1
 - Discovering ONTAP clusters 1
 - Provisioning storage for ONTAP clusters 2
 - Tier on-prem data to the cloud 3

Manage ONTAP clusters

Discovering ONTAP clusters

Cloud Manager can discover the ONTAP clusters in your on-premises environment, in a NetApp Private Storage configuration, and in the IBM Cloud. Discovering an ONTAP cluster enables you to provision storage, replicate data, and tier cold data from an on-prem cluster to the cloud.

Before you begin

You must have the cluster management IP address and the password for the admin user account to add the cluster to Cloud Manager.

Cloud Manager discovers ONTAP clusters using HTTPS. If you use custom firewall policies, they must meet the following requirements:

- The Cloud Manager host must allow outbound HTTPS access through port 443.

If Cloud Manager is in AWS, all outbound communication is allowed by the predefined security group.

- The ONTAP cluster must allow inbound HTTPS access through port 443.

The default "mgmt" firewall policy allows inbound HTTPS access from all IP addresses. If you modified this default policy, or if you created your own firewall policy, you must associate the HTTPS protocol with that policy and enable access from the Cloud Manager host.

Steps

1. On the Working Environments page, click **Discover** and select **ONTAP Cluster**.
2. On the **ONTAP Cluster Details** page, enter the cluster management IP address, the password for the admin user account, and the location of the cluster.

ONTAP Cluster Details

Provide a few details about your ONTAP cluster so Cloud Manager can discover it.

Cluster Details

Cluster management IP address

User name

Password

Cluster Location



On Premises



IBM Cloud



Microsoft Azure



Amazon Web Services



Google Cloud

3. On the Details page, enter a name and description for the working environment, and then click **Go**.

Result

Cloud Manager discovers the cluster. You can now create volumes, replicate data to and from the cluster, and launch OnCommand System Manager to perform advanced tasks.``

Provisioning storage for ONTAP clusters

After you discover your ONTAP cluster from Cloud Manager, you can open the working environment to provision storage.

Creating volumes for ONTAP clusters

Cloud Manager enables you to provision NFS and CIFS volumes on ONTAP clusters.

Before you begin

NFS or CIFS must be set up on the cluster. You can set up NFS and CIFS using System Manager or the CLI.

About this task

You can create volumes on existing aggregates. You cannot create new aggregates from Cloud Manager.

Steps

1. On the Working Environments page, double-click the name of the ONTAP cluster on which you want to provision volumes.
2. Click **Add New Volume**.
3. On the Create New Volume page, enter details for the volume, and then click **Create**.

Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.

Field	Description
Usage Profile	Usage profiles define the NetApp storage efficiency features that are enabled for a volume.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.

Replicating data

You can replicate data between Cloud Volumes ONTAP systems and ONTAP clusters by choosing a one-time data replication, which can help you move data to and from the cloud, or a recurring schedule, which can help with disaster recovery or long-term retention.

[Click here for more details.](#)

Using ONTAP as persistent storage

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

[Click here for more details.](#)

Tier on-prem 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 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 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

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.

Cost

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. [Learn how licensing works](#).

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

Cloud Tiering integration with Cloud Manager

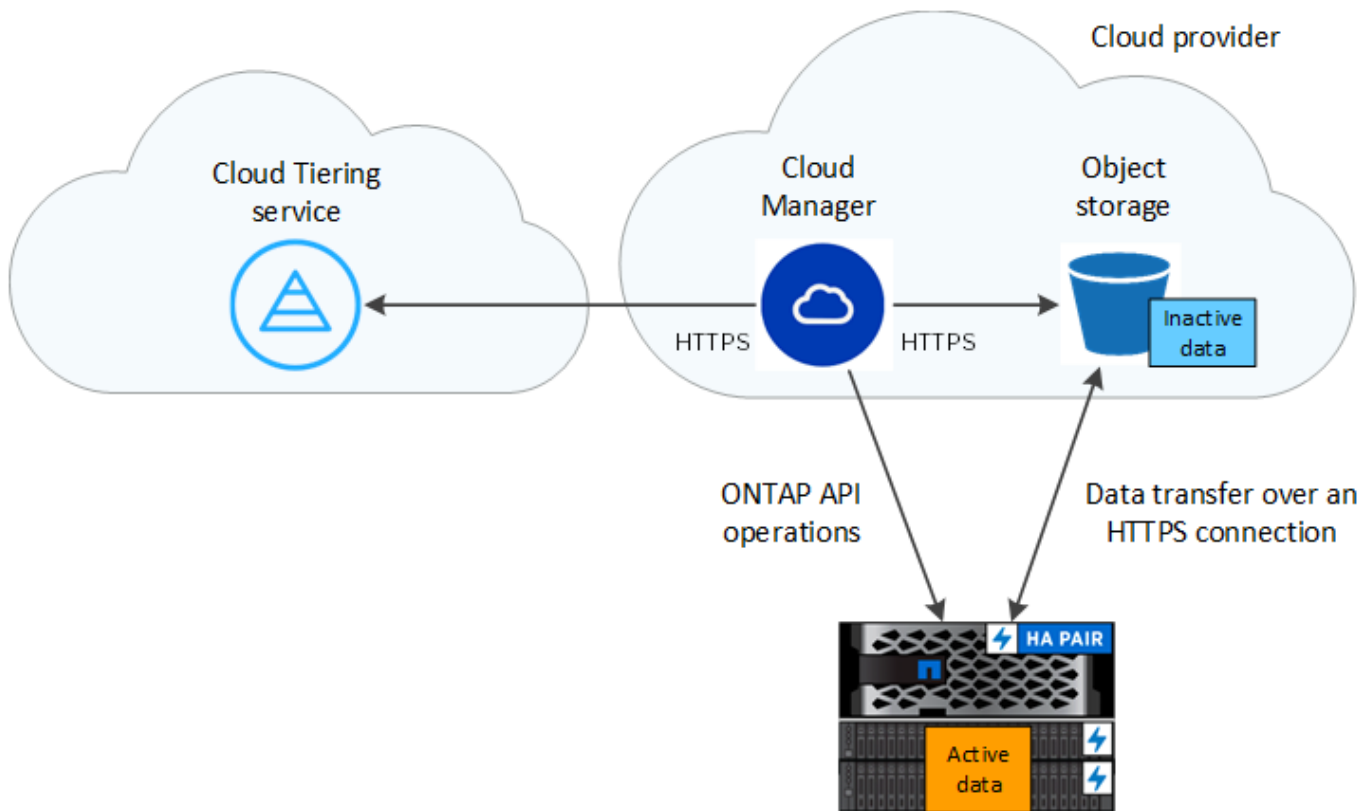
The Cloud Tiering service is available from [NetApp Cloud Central](#) as a standalone service. But it's also integrated into Cloud Manager to make it easier for you to manage your hybrid cloud storage from a single interface. The integration with Cloud Manager also reduces complexity because there's no need to deploy the NetApp Service Connector because it's part of Cloud Manager.

If you switch between Cloud Manager and [the interface for Cloud Tiering](#), you'll see the same set of clusters. Think of it as the same application presented through different interfaces.

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 Cloud Manager.

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.



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* moved to the cloud tier. 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).



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

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.
- Cloud Manager installed in an AWS VPC or on your premises.
- Networking for Cloud Manager that enables an outbound HTTPS connection to the ONTAP cluster, to S3 storage, 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 Amazon S3.

3

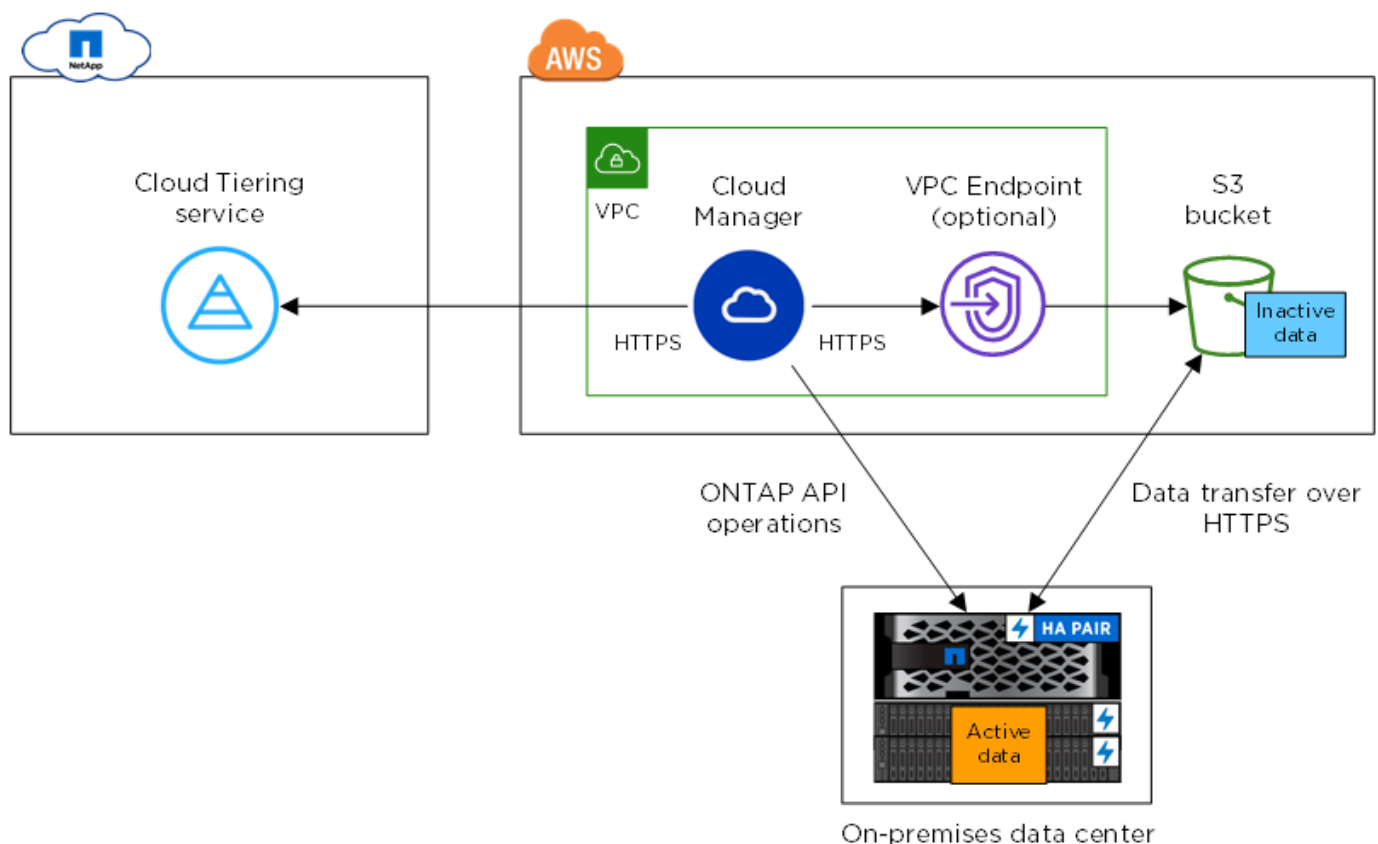
Set up licensing

Pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both. Licensing isn't available from within Cloud Manager, [but you can go directly to the Cloud Tiering service to set it up](#).

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 Cloud Manager and S3 is for object storage setup only. Cloud Manager 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 Cloud Manager, 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.

Preparing networking for Cloud Manager

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

Steps

1. Ensure that the network where Cloud Manager 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 Cloud Manager 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 Cloud Manager 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

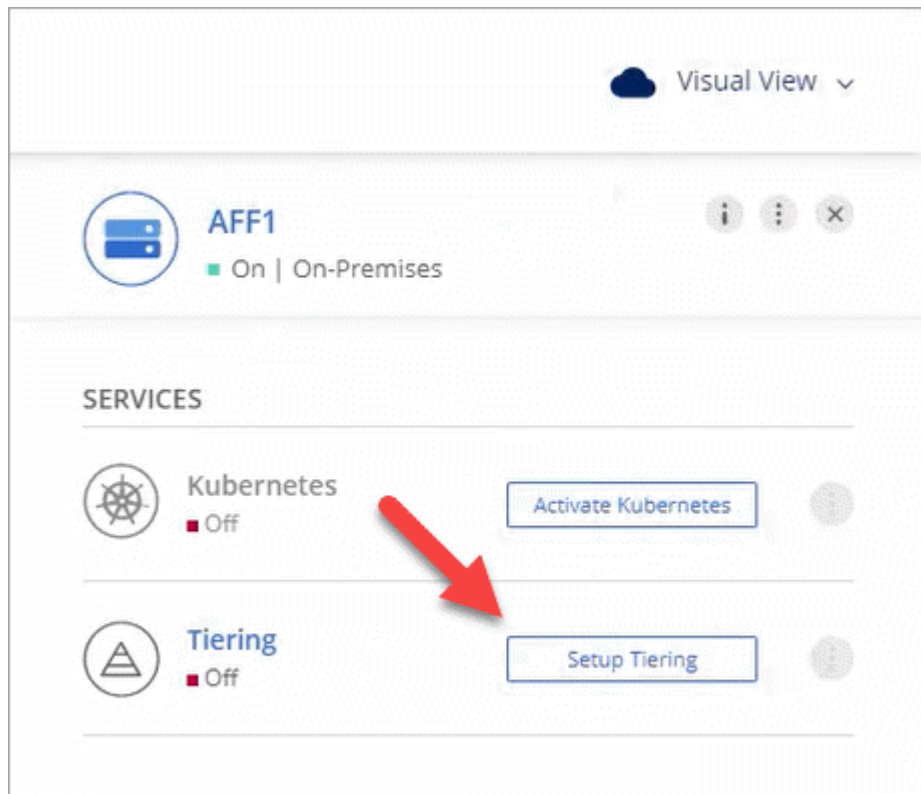
After you prepare your AWS environment, start tiering inactive data from your first cluster.

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 Service 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. Click the  icon, select a tiering policy, optionally adjust the cooling days, and click **Apply**.

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

Tier Volumes							
Learn how much you can save with each Tiering Policy							
1 - 3 of 3 Volumes							
Volume Name	SVM Name	Volume Size	Used Size	Cold Data		Tier Status [3]	Tiering Policy
vol1	svm_AFF1	200 GB	3.8 MB	2.66 ...	70 %	✓ Tiered Volume	All user data
vol2	svm_AFF1	400 GB	2.59 MB	1.81 ...	70 %	✓ Tiered Volume	Cold user data
vol3	svm_AFF1	325 GB	2.59 MB	0 B	0 %	✓ 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.
- Cloud Manager installed in an Azure VNet.
- Networking for Cloud Manager 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

Log in to [NetApp Cloud Central](#), start a free trial of the Cloud Tiering service, and click **Let's Start, Discover Your First Cluster**.



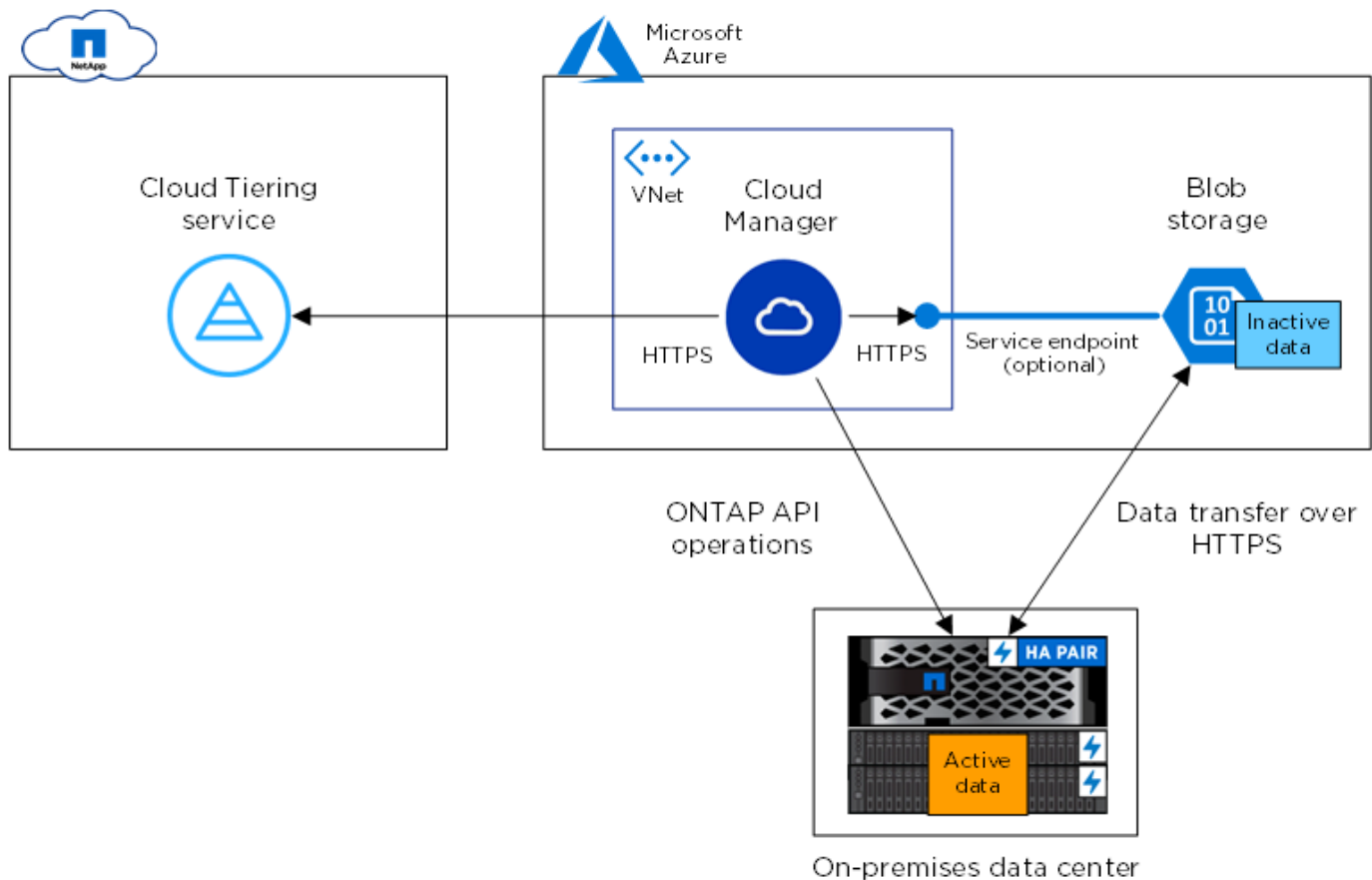
Set up licensing

Pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both. Licensing isn't available from within Cloud Manager, [but you can go directly to the Cloud Tiering service to set it up](#).

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 Cloud Manager 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.

Preparing networking for Cloud Manager

Ensure that Cloud Manager has the required networking connections.

Steps

1. Ensure that the VNet where Cloud Manager 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 Cloud Manager and Blob storage to stay in your virtual private network.

Tiering inactive data from your first cluster to Azure Blob storage

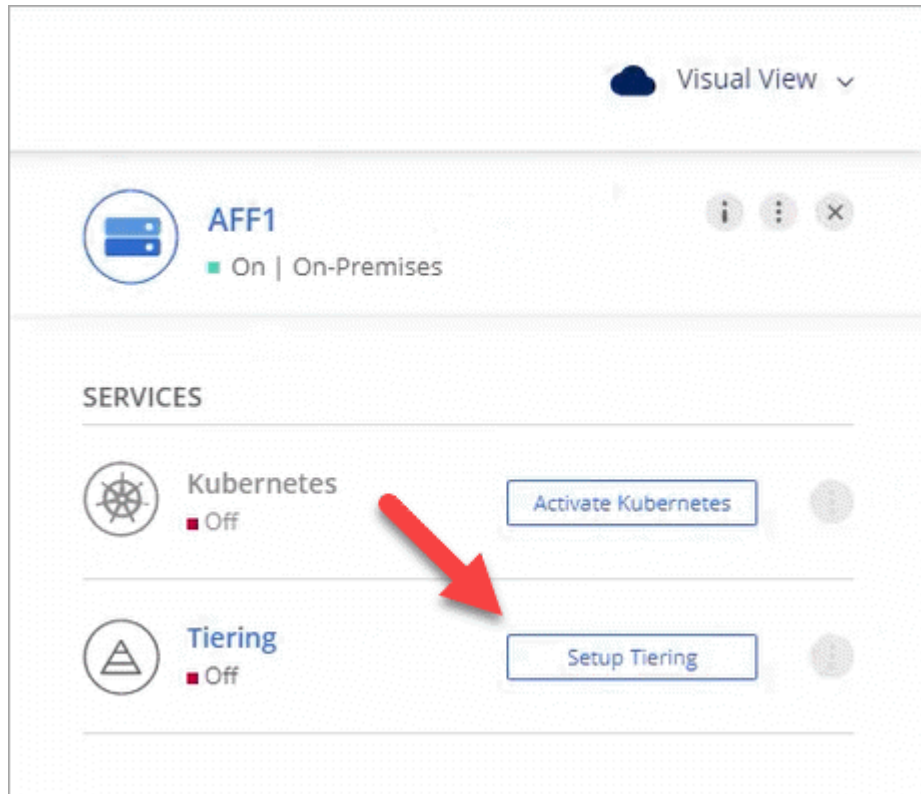
After you prepare your Azure environment, start tiering inactive data from your first cluster.

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. **Azure Container**: Add a new Blob container or select an existing container and click **Continue**.
 - b. **Access Tier**: Select the access tier that you want to use for the tiered data and click **Continue**.
 - c. **Cluster Network**: Select the IPspace that ONTAP should use to connect to object storage and click **Continue**.

Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your 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							Learn how much you can save with each Tiering Policy	
1 - 3 of 3 Volumes								
Volume Name	SVM Name	Volume Size	Used Size	Cold Data		Tier Status [3]	Tiering Policy	
vol1	svm_AFF1	200 GB	3.8 MB	2.66 ...	70 %	✓ Tiered Volume	All user data	
vol2	svm_AFF1	400 GB	2.59 MB	1.81 ...	70 %	✓ Tiered Volume	Cold user data	
vol3	svm_AFF1	325 GB	2.59 MB	0 B	0 %	✓ 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.
- Cloud Manager installed in a Google Cloud Platform VPC.
- Networking for Cloud Manager 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

Select an on-prem working environment, click **Setup Tiering** and follow the prompts to tier data to

Google Cloud Storage.

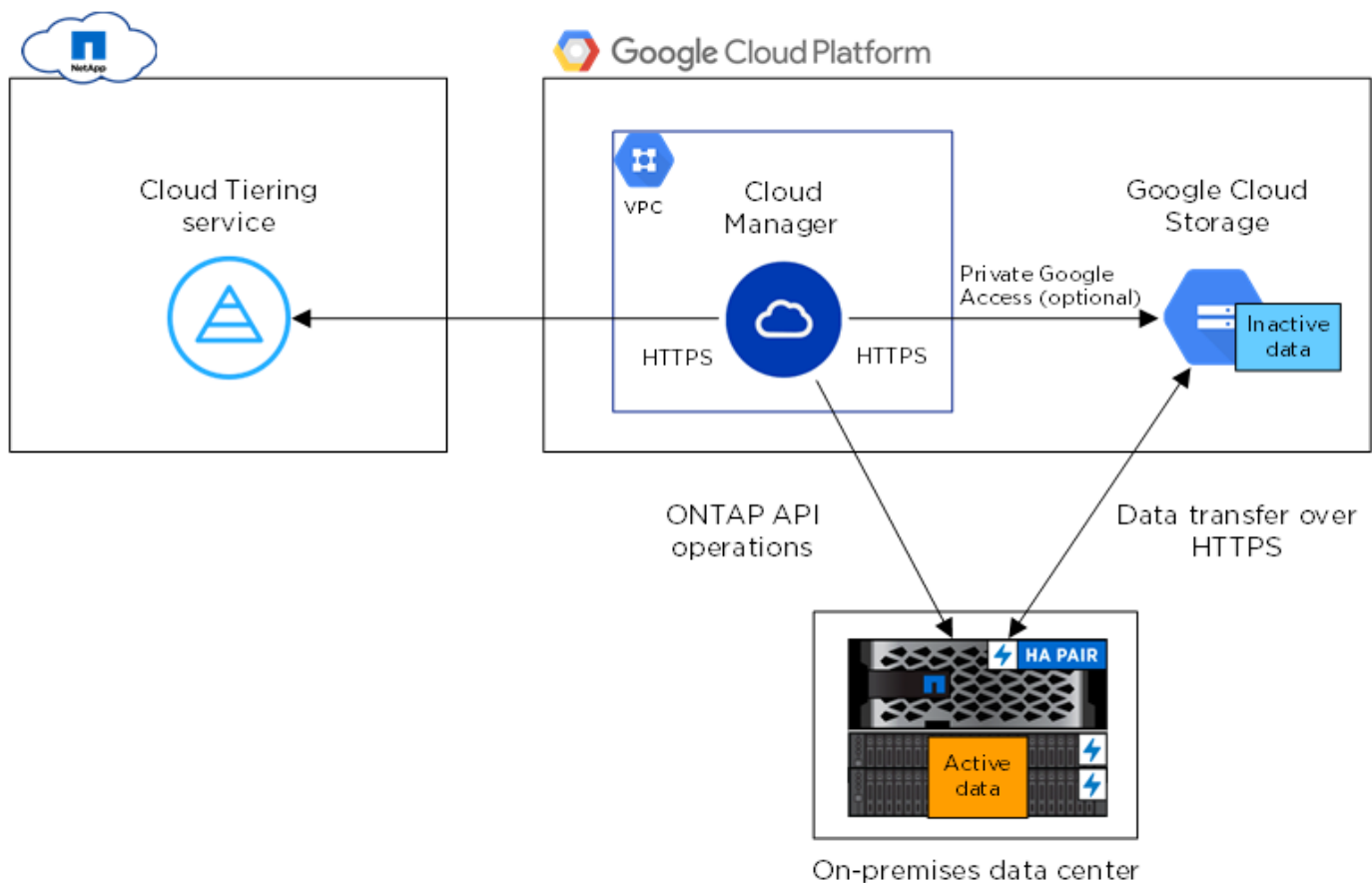
3 Set up licensing

Pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both. Licensing isn't available from within Cloud Manager, [but you can go directly to the Cloud Tiering service to set it up](#).

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 Cloud Manager 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.

Preparing networking for Cloud Manager

Ensure that Cloud Manager has the required networking connections.

Steps

1. Ensure that the VPC where Cloud Manager 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 Cloud Manager 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

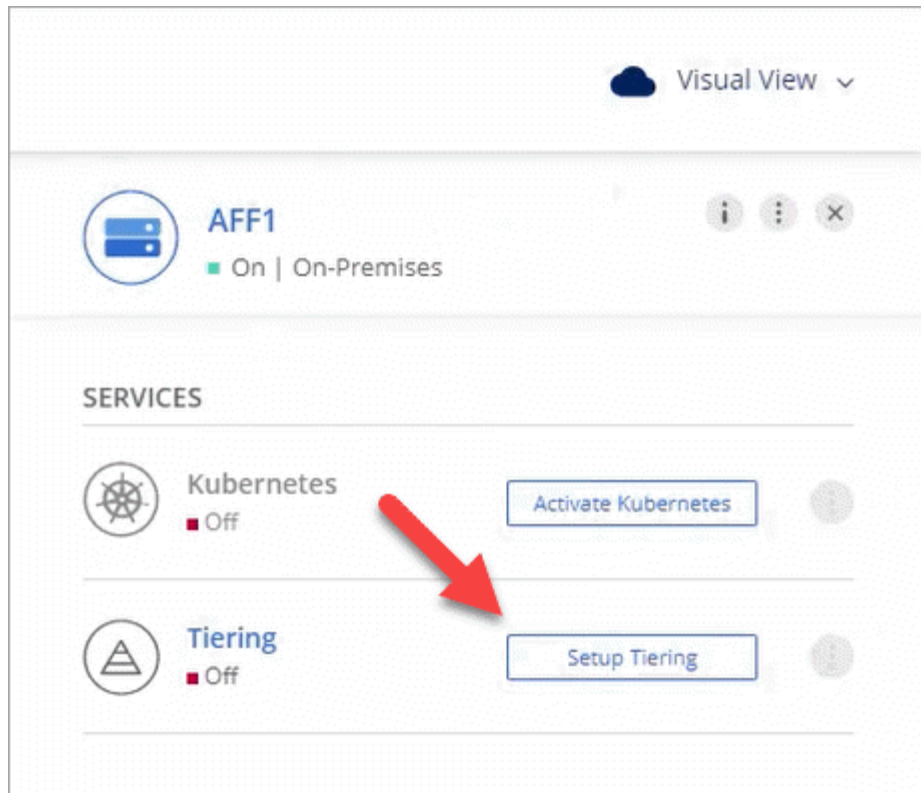
After you prepare your Google Cloud environment, start tiering inactive data from your first cluster.

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. Click the  icon, select a tiering policy, optionally adjust the cooling days, and click **Apply**.

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

Tier Volumes							Learn how much you can save with each Tiering Policy	
1 - 3 of 3 Volumes								
Volume Name	SVM Name	Volume Size	Used Size	Cold Data		Tier Status [3]	Tiering Policy	
vol1	svm_AFF1	200 GB	3.8 MB	2.66 ...	70 %	✓ Tiered Volume	All user data	
vol2	svm_AFF1	400 GB	2.59 MB	1.81 ...	70 %	✓ Tiered Volume	Cold user data	
vol3	svm_AFF1	325 GB	2.59 MB	0 B	0 %	✓ 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.



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.
- Cloud Manager installed on your premises.
- Networking for Cloud Manager that enables an outbound HTTPS connection to the ONTAP cluster, to StorageGRID, and to the Cloud Tiering service.



Set up tiering

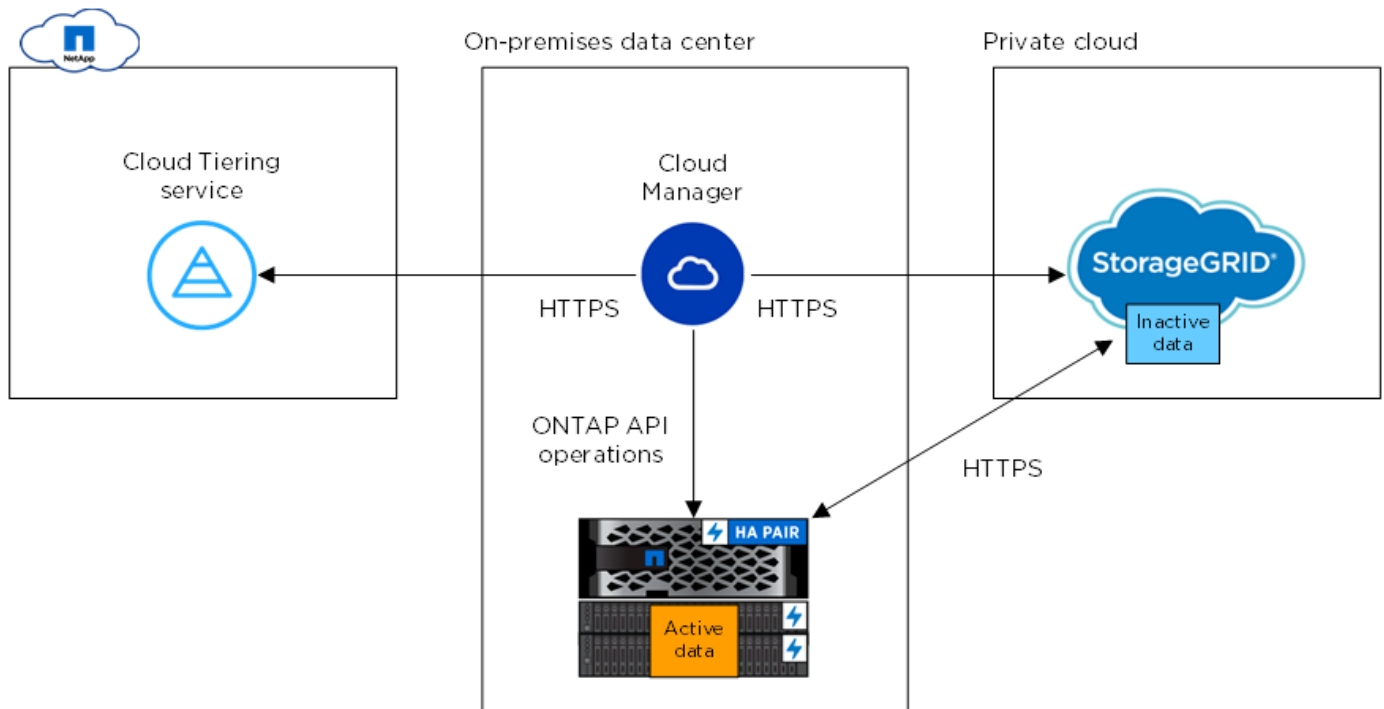
Select an on-prem working environment, click **Setup Tiering** and follow the prompts to tier data to

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 Cloud Manager 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 Cloud Manager, 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.

Preparing networking for Cloud Manager

Ensure that Cloud Manager has the required networking connections.

Steps

1. Ensure that the network where Cloud Manager 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

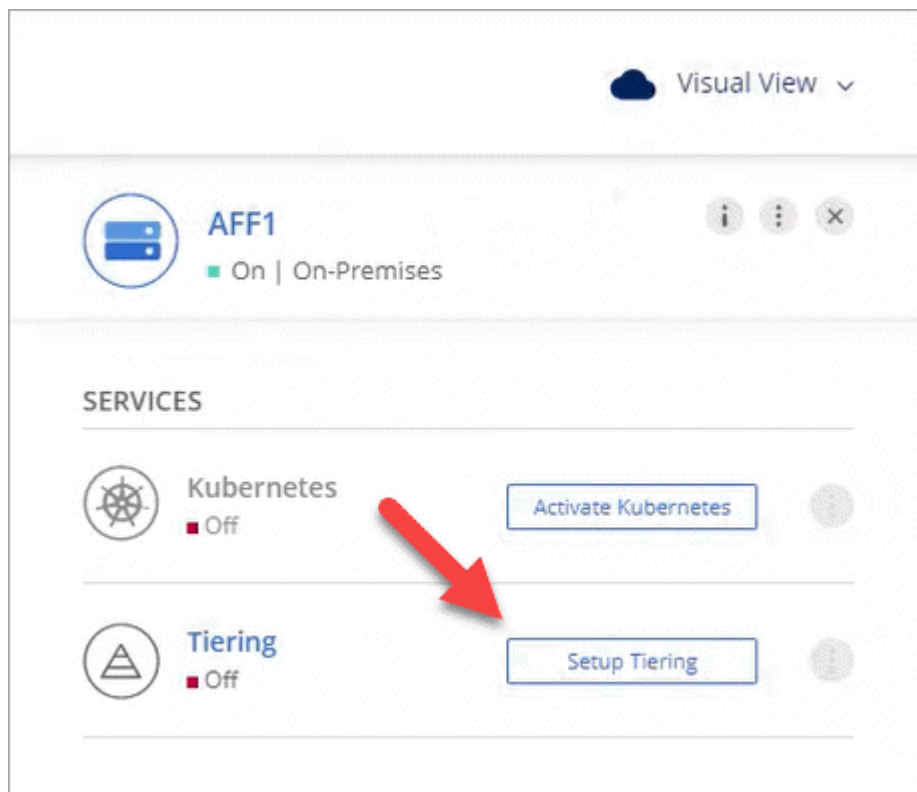
After you prepare your environment, start tiering inactive data from your first cluster.

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							
Learn how much you can save with each Tiering Policy							
1 - 3 of 3 Volumes							
Volume Name	SVM Name	Volume Size	Used Size	Cold Data	Tier Status [3]		Tiering Policy
vol1	svm_AFF1	200 GB	3.8 MB	2.66 ... 70 %	✓ Tiered Volume		All user data
vol2	svm_AFF1	400 GB	2.59 MB	1.81 ... 70 %	✓ Tiered Volume		Cold user data
vol3	svm_AFF1	325 GB	2.59 MB	0 B 0 %	✓ Tiered Volume		Cold snapshots

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. [Learn how licensing works](#).

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'd like to purchase a FabricPool license, [learn how to get one and install it on the cluster](#).

If you want to pay-as-you-go, then you'll need to set up licensing directly from the Cloud Tiering service, which is accessible from Cloud Central. Licensing for Cloud Tiering isn't available through Cloud Manager at this time.



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

Steps to set up a PAYGO subscription

1. Log in to [NetApp Cloud Central](#).
2. From the Fabric View, click **Go to Cloud Tiering**.
3. Now that you're in the Cloud Tiering service, [follow the steps in the Cloud Tiering documentation](#) to subscribe from your cloud provider's marketplace.


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 **OnPrem Tiering**.
2. From the **Cluster Dashboard**, click **Tier Volumes** for the cluster.
3. 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							
Learn how much you can save with each Tiering Policy							
1 - 3 of 3 Volumes							
Volume Name	SVM Name	Volume Size	Used Size	Cold Data	Tier Status [3]		Tiering Policy
vol1	svm_AFF1	200 GB	3.8 MB	2.66 ... 70 %	✓ Tiered Volume		All user data
vol2	svm_AFF1	400 GB	2.59 MB	1.81 ... 70 %	✓ Tiered Volume		Cold user data
vol3	svm_AFF1	325 GB	2.59 MB	0 B 0 %	✓ Tiered Volume		Cold snapshots




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.

4. When you're done, click **Close**.

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 **OnPrem 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**.

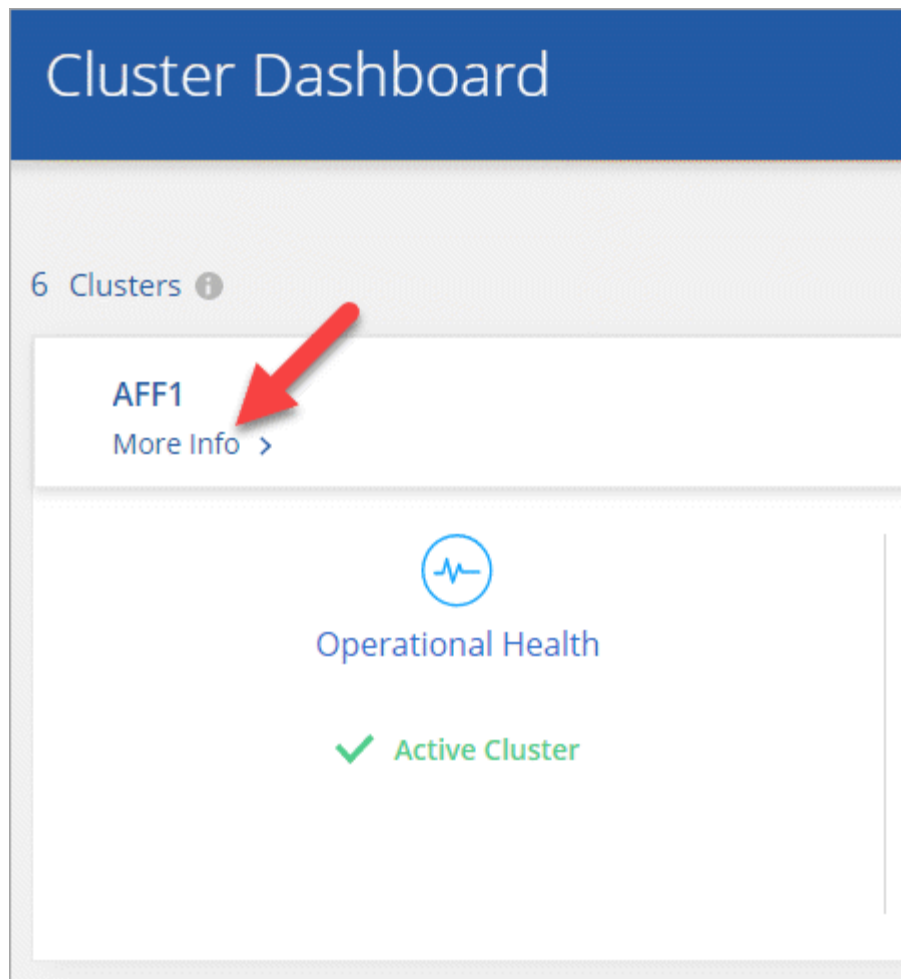
[Learn more about volume tiering policies.](#)

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.

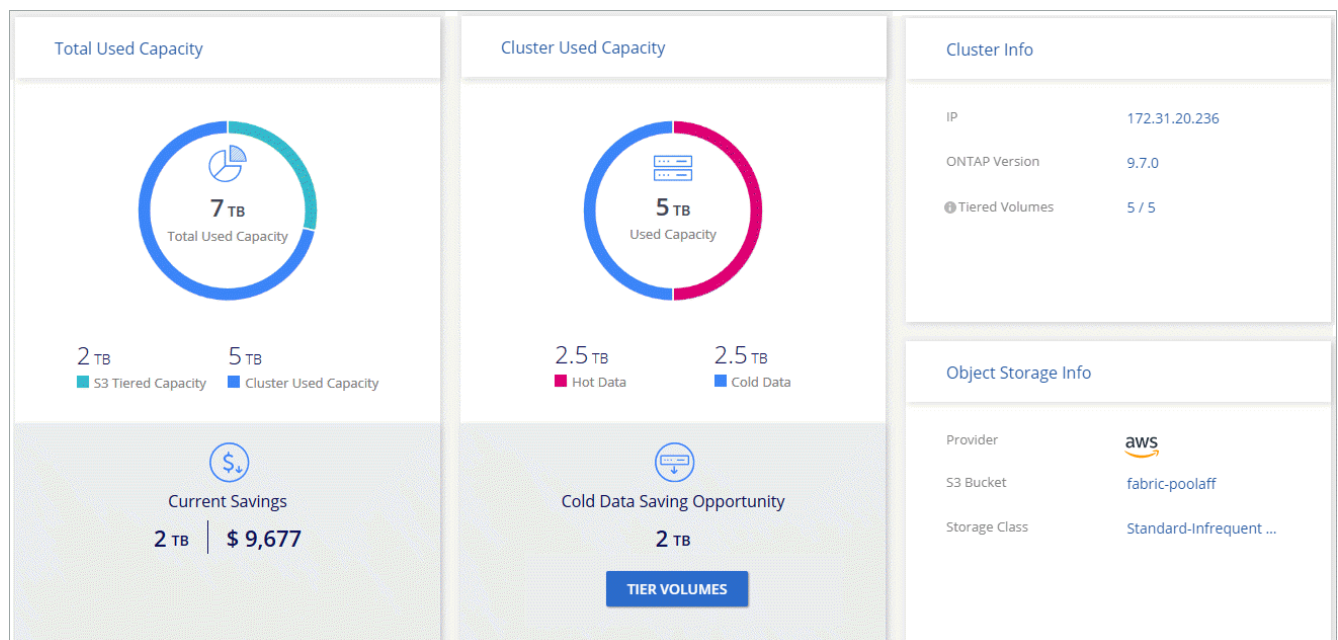
Steps

1. At the top of Cloud Manager, click **OnPrem 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."

Unknown Cluster		Tiering Setup Status
		Tiering hasn't been setup through Cloud Tiering
 Operational Health	 Current Savings	 Saving Opportunities
✖ Failed ⓘ	No Available Data	No Available Data

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.

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.

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.

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.

Cloud Manager

The following questions relate to Cloud Manager.

Where does Cloud Manager need to be installed?

- When tiering data to S3, Cloud Manager can reside in an AWS VPC or on your premises.
- When tiering data to Blob storage, Cloud Manager must reside in an Azure VNet.
- When tiering data to Google Cloud Storage, Cloud Manager must reside in a Google Cloud Platform VPC.
- When tiering data to StorageGRID, Cloud Manager must reside on an on premises Linux host.

What's the difference between Cloud Manager and a Service Connector?

There's no difference, really. A Service Connector is part of Cloud Manager.

You might be familiar with the Service Connector term if you've accessed the Cloud Tiering service directly from NetApp Cloud Central. Cloud Tiering prompts you to deploy a Service Connector to discover your on-prem clusters. That's not necessary when you use Cloud Tiering from within Cloud Manager because Cloud Manager acts as the Service Connector—it communicates with ONTAP clusters to discover information about active and inactive data, and to set up data tiering.

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).
- Cloud Manager 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

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.