# Table of Contents

Cloud Tiering documentation ................................. 1  
What’s new with Cloud Tiering ................................. 2  
  6 November 2022 .............................................. 2  
  19 September 2022 ........................................... 2  
  3 August 2022 ............................................... 2  
  3 May 2022 ................................................ 3  
  4 April 2022 ................................................. 3  
  2 September 2021 ............................................. 3  
Get started ..................................................... 4  
  Learn about Cloud Tiering ................................. 4  
  Tier on-prem data to the cloud ......................... 9  
  Set up licensing for Cloud Tiering .................. 43  
  Cloud Tiering technical FAQ ............................ 50  
Use Cloud Tiering ............................................. 60  
  Managing data tiering from your clusters .......... 60  
  Managing object storage used for data tiering ...... 67  
  Measure network latency and throughput performance 73  
  Get an overview of data tiering from your clusters 74  
Reference ......................................................... 75  
  Supported S3 storage classes and regions .......... 75  
  Supported Azure Blob access tiers and regions .... 76  
  Supported Google Cloud storage classes and regions 77  
Knowledge and support ......................................... 79  
  Register for support ......................................... 79  
  Get help ....................................................... 82  
Legal notices ...................................................... 86  
  Copyright .................................................... 86  
  Trademarks ................................................ 86  
  Patents ...................................................... 86  
  Privacy policy .............................................. 86  
  Open source ............................................... 86
What’s new with Cloud Tiering

Learn what’s new in Cloud Tiering.

6 November 2022

Drag and drop to enable Cloud Tiering to Azure Blob, Google Cloud Storage, and StorageGRID

If the Azure Blob, Google Cloud Storage, or StorageGRID tiering destination exists as a working environment on the Canvas, you can drag your on-prem ONTAP working environment onto the destination to initiate the Tiering setup wizard.

19 September 2022

Tiering wizard enables you to configure AWS PrivateLink when tiering to S3 storage

In previous releases it was very time-consuming to provide this secure way of connecting your cluster to an S3 bucket through a VPC endpoint. Now you can follow the prerequisite steps to configure your system for a private connection using a VPC endpoint interface, and then you can select the PrivateLink during the Tiering setup wizard in the Networking page.

Review the requirements and steps to tier inactive data to Amazon S3.

Drag and drop to enable Cloud Tiering to Amazon S3

If the Amazon S3 tiering destination exists as a working environment on the Canvas, you can drag your on-prem ONTAP working environment onto the destination to initiate the Tiering setup wizard.

Choose the tiering behavior when removing the mirror object store in a MetroCluster configuration

When removing the mirror object store from a MetroCluster configuration, you’ll be prompted whether you want to remove the primary object store as well. You can choose to keep the primary object store attached to the aggregate, or to remove it.

3 August 2022

Ability to configure additional object stores for other aggregates in your cluster

The Cloud Tiering UI has added a new set of pages for object storage configuration. You can add new object stores, connect multiple object stores to an aggregate for FabricPool Mirroring, swap the primary and mirror object stores, delete object store connections to aggregates, and more. Learn more about the new object storage functionality.

Cloud Tiering license support for MetroCluster configurations

Cloud Tiering licenses can now be shared with your clusters that are in MetroCluster configurations. You no longer have to use the deprecated FabricPool licenses for these scenarios. This makes it easier to use the
"floating" Cloud Tiering licenses on more of your clusters. See how to license and configure these types of clusters.

3 May 2022

Cloud Tiering license support for additional cluster configurations

Cloud Tiering licenses can now be shared with your clusters that are in Tiering Mirror configurations (not including MetroCluster configurations) and with clusters that are tiered to IBM Cloud Object Storage. You no longer have to use the deprecated FabricPool licenses for these scenarios. This makes it easier to use the "floating" Cloud Tiering licenses on more of your clusters. See how to license and configure these types of clusters.

4 April 2022

Amazon S3 Glacier Instant Retrieval storage class is now available

When setting up Cloud Tiering, now you can configure a lifecycle rule so your inactive data transitions from the Standard storage class to Glacier Instant Retrieval after a certain number of days. This will help reduce your AWS infrastructure costs. See the supported S3 storage classes.

Cloud Tiering has been fully qualified on ONTAP Select systems

In addition to tiering data from your AFF and FAS systems, now you can tier inactive data from your ONTAP Select systems to cloud storage.

2 September 2021

Cloud Tiering BYOL license replaces FabricPool license

A new Cloud Tiering license is now available for tiering configurations that are supported within BlueXP using the Cloud Tiering service. It is a floating license that you can use across multiple on-premises ONTAP clusters. The FabricPool license that you may have used in the past is retained only for configurations that aren’t supported within BlueXP.

Learn more about the new Cloud Tiering license.

Tier inactive data from on-prem ONTAP clusters to S3-compatible object storage

Now you can tier inactive data to any Object Storage service which uses the Simple Storage Service (S3) protocol. See how to tier data to S3-compatible object storage.
Get started

Learn about Cloud Tiering

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

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

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

Cloud Tiering can be configured for single-node clusters, HA-configured clusters, clusters in Tiering Mirror configurations, and MetroCluster configurations using FabricPool Mirror. Cloud Tiering licenses are shared among all of your clusters.

Features

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

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

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

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

Supported object storage providers

You can tier inactive data from an on-premises ONTAP system to the following object storage providers:
• Amazon S3
• Microsoft Azure Blob
• Google Cloud Storage
• S3-compatible object storage
• NetApp StorageGRID

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

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

Object storage tiers

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

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

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

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

Pricing and licenses

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

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

View pricing details.

30-day free trial

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

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

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

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

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

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

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

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

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

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

**Annual contract**

Cloud Tiering offers an annual contract when tiering inactive data to Amazon S3. It’s available in 1-, 2-, or 3-year terms.

Annual contracts are not currently supported when tiering to Azure or GCP.

**Bring your own license**

Bring your own license by purchasing a Cloud Tiering license from NetApp. You can purchase 1-, 2-, or 3-year term licenses and specify any amount of tiering capacity. The BYOL Cloud Tiering license is a floating license that you can use across multiple on-premises ONTAP clusters. The total tiering capacity that you define in your Cloud Tiering license can be used by all of your on-prem clusters.

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

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

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

**How Cloud Tiering works**

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

The following image shows the relationship between each component:
At a high level, Cloud Tiering works like this:

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

**Volume tiering policies**

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

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

**No Policy (None)**

- Keeps the data on a volume in the performance tier, preventing it from being moved to the cloud tier.
Cold snapshots (Snapshot only)
ONTAP tiers cold Snapshot blocks in the volume that are not shared with the active file system to object storage. If read, cold data blocks on the cloud tier become hot and are moved to the performance tier.

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

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

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

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

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

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

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

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

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

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

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

- Cloud Backup is similarly affected by volumes set with a tiering policy. See tiering policy considerations with Cloud Backup.
All DP user data (Backup)

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

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

Tier on-prem data to the cloud

Tiering data from on-premises ONTAP clusters to Amazon S3

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

Quick start

Get started quickly by following these steps. Details for each step are provided in the following sections in this topic.

1. Identify the configuration method you’ll use

Choose whether you’ll connect your on-premises ONTAP cluster directly to AWS S3 over the public internet, or whether you’ll use a VPN or AWS Direct Connect and route traffic through a private VPC Endpoint interface to AWS S3.

See the available connection methods.

2. Prepare your BlueXP Connector

If you already have a Connector deployed in your AWS VPC or on your premises, then you’re all set. If not, then you’ll need to create a Connector to tier ONTAP data to AWS S3 storage. You’ll also need to customize network settings for the Connector so that it can connect to AWS S3.

See how to create a Connector and how to define required network settings.

3. Prepare your on-premises ONTAP cluster

Discover your ONTAP cluster in BlueXP, verify that the cluster meets minimum requirements, and customize network settings so the cluster can connect to AWS S3.

See how to get your on-premises ONTAP cluster ready.

4. Prepare Amazon S3 as your tiering target

Set up permissions for the Connector to create and manage the S3 bucket. You’ll also need to set up permissions for the on-premises ONTAP cluster so it can read and write data to the S3 bucket.

See how to set up permissions for the Connector and for your on-prem cluster.
Enable Cloud Tiering on the system
Select an on-prem working environment, click **Enable** for the Tiering service, and follow the prompts to tier data to Amazon S3.

See how to enable Tiering for your volumes.

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 BlueXP 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 BlueXP Digital Wallet.

Network diagrams for connection options
There are two connection methods you can use when configuring tiering from on-premises ONTAP systems to AWS S3.

- Public connection - Directly connect the ONTAP system to AWS S3 using a public S3 endpoint.
- Private connection - Use a VPN or AWS Direct Connect and route traffic through a VPC Endpoint interface that uses a private IP address.

The following diagram shows the **public connection** method and the connections that you need to prepare between the components. You can use a Connector that you’ve installed on your premises, or a Connector that you’ve deployed in the AWS VPC.
The following diagram shows the **private connection** method and the connections that you need to prepare between the components. You can use a Connector that you’ve installed on your premises, or a Connector that you’ve deployed in the AWS VPC.

Communication between a Connector and S3 is for object storage setup only.
Prepare your Connector

The BlueXP Connector is the main software for BlueXP functionality. A Connector is required to tier your inactive ONTAP data.

Creating or switching Connectors

If you already have a Connector deployed in your AWS VPC or on your premises, then you're all set. If not, then you'll need to create a Connector in either of those locations to tier ONTAP data to AWS S3 storage. You can’t use a Connector that’s deployed in another cloud provider.

- Learn about Connectors
- Getting started with Connectors
- Installing a Connector in AWS
- Installing a Connector in your premises

Connector networking requirements

- Ensure that the network where the Connector is installed enables the following connections:
  - An outbound internet connection over port 443 (HTTPS) to the Cloud Tiering service
  - An HTTPS connection over port 443 to your S3 object storage (see the list of endpoints)
  - An HTTPS connection over port 443 to your ONTAP cluster management LIF
- Ensure that the Connector has permissions to manage the S3 bucket
- 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 (a private connection), you’ll need to enable a VPC Endpoint interface to S3. See how to set up a VPC endpoint interface.

Prepare your ONTAP cluster

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

ONTAP requirements

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 9.2 or later
- ONTAP 9.7 or later is required if you plan to use an AWS PrivateLink connection to object storage

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 the 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.

**Required application access parameter**

The cluster admin user must have “console” Application access. You can verify this using the ONTAP command `security login show`. "console" should appear in the Application column for the "admin" user. Use the `security login create` command to add console application access if necessary. See the "security login" commands for details.

**Cluster networking requirements**

- The cluster requires an inbound HTTPS connection from the Connector to the cluster management LIF. 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. These intercluster LIFs must be able to access the object store.

  The cluster initiates an outbound HTTPS connection over port 443 from the intercluster LIFs to Amazon S3 storage for tiering operations. ONTAP reads and writes data to and from object storage — the object storage never initiates, it just responds.

- The intercluster LIFs must be associated with the IPspace that ONTAP should use to connect to object storage. Learn more about IPspaces.

  When you set up Cloud Tiering, you are prompted for the IPspace to use. You should choose the IPspace that these LIFs are associated with. That might be the "Default" IPspace or a custom IPspace that you created.

  If you use are using a different IPspace than "Default", then you might need to create a static route to get access to the object storage.

  All intercluster LIFs within the IPspace must have access to the object store. If you can’t configure this for the current IPspace, then you’ll need to create a dedicated IPspace where all intercluster LIFs have access to the object store.

- If you are using a Private VPC Interface Endpoint in AWS for the S3 connection, then in order for HTTPS/443 to be used, you’ll need to load the S3 endpoint certificate into the ONTAP cluster. See how to set up a VPC endpoint interface and load the S3 certificate.

- Ensure that your ONTAP cluster has permissions to access the S3 bucket.

**Discover your ONTAP cluster in BlueXP**

You need to discover your on-premises ONTAP cluster in BlueXP before you can start tiering cold data to object storage. You’ll need to know the cluster management IP address and the password for the admin user account to add the cluster.

Learn how to discover a cluster.

**Prepare your AWS environment**

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.

Set up S3 permissions

You’ll need to configure two sets of permissions:

• Permissions for the Connector to create and manage the S3 bucket.

• Permissions for the on-premises ONTAP cluster so it can read and write data to the S3 bucket.

Steps

1. Confirm that these S3 permissions are part of the IAM role that provides the Connector with permissions. They should have been included by default when you first deployed the Connector. If not, you’ll need to add the missing permissions. See the AWS Documentation: Editing IAM policies.

2. When activating the service, the Tiering wizard will prompt you to enter an access key and secret key. These credentials are passed to the ONTAP cluster so that ONTAP can tier data to the S3 bucket. For that, you’ll need to create an IAM user with the following permissions:

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

See the AWS Documentation: Creating a Role to Delegate Permissions to an IAM User for details.

3. Create or locate the 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

Configure your system for a private connection using a VPC endpoint interface

If you plan to use a standard public internet connection, then all the permissions are set by the Connector and there is nothing else you need to do. This type of connection is shown in the first diagram above.

If you want to have a more secure connection over the internet from your on-prem data center to the VPC, there’s an option to select an AWS PrivateLink connection in the Tiering activation wizard. It’s required if you plan to use a VPN or AWS Direct Connect to connect your on-premises system through a VPC Endpoint interface that uses a private IP address. This type of connection is shown in the second diagram above.
1. Create an Interface endpoint configuration using the Amazon VPC console or the command line. See details about using AWS PrivateLink for Amazon S3.

2. Modify the security group configuration that’s associated with the BlueXP Connector. You must change the policy to "Custom" (from "Full Access"), and you must add the required S3 Connector permissions as shown earlier.

   ![Security Group Configuration](image)

   If you’re using port 80 (HTTP) for communication to the private endpoint, you’re all set. You can enable Cloud Tiering on the cluster now.

   If you’re using port 443 (HTTPS) for communication to the private endpoint, you must copy the certificate from the VPC S3 endpoint and add it to your ONTAP cluster, as shown in the next 4 steps.

3. Obtain the DNS name of the endpoint from the AWS Console.
4. Obtain the certificate from the VPC S3 endpoint. You do this by logging into the VM that hosts the BlueXP Connector and running the following command. When entering the DNS name of the endpoint, add "bucket" to the beginning, replacing the "*":

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
```

5. From the output of this command, copy the data for the S3 certificate (all data between, and including, the BEGIN / END CERTIFICATE tags):

```
Certificate chain
  0 s:/CN=s3.us-west-2.amazonaws.com`
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADB... 
GqvbOz/oO2NWLLFCqI+xmkLcMiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo= 
-----END CERTIFICATE-----
```

6. Log into the ONTAP cluster CLI and apply the certificate you copied using the following command (substitute your own storage VM name):
Tier 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.

   If the Amazon S3 tiering destination exists as a working environment on the Canvas, you can drag the cluster onto the working environment to initiate the setup wizard.

3. **Define Object Storage Name**: Enter a name for this object storage. It must be unique from any other object storage you may be using with aggregates on this cluster.

4. **Select Provider**: Select **Amazon Web Services** and click **Continue**.
5. Complete the sections on the **Create Object Storage** page:

   a. **S3 Bucket**: Add a new S3 bucket or select an existing S3 bucket that starts with the prefix `fabric-pool`, select the bucket region, 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**: 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. **Networking**: Enter the networking details and click **Continue**.

Select the IPspace in the ONTAP cluster where the volumes you want to tier reside. The intercluster LIFs for this IPspace must have outbound internet access so that they can connect to your cloud provider’s object storage.

 Optionally, choose whether you’ll use an AWS PrivateLink that you have previously configured. See the setup information above.

A dialog box is displayed to help guide you through the endpoint configuration.

6. 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.
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 object storage.

**What’s next?**

Be sure to subscribe to the Cloud Tiering service.

You can review information about the active and inactive data on the cluster. Learn more about managing your tiering settings.

You can also create additional object storage in cases where you may want to tier data from certain aggregates on a cluster to different object stores. Or if you plan to use FabricPool Mirroring where your tiered data is replicated to an additional object store. Learn more about managing object stores.

**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 BlueXP, 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 BlueXP 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 BlueXP 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

Required application access parameter

The cluster admin user must have “console” Application access. You can verify this using the ONTAP command `security login show`. "console" should appear in the Application column for the "admin" user. Use the `security login create` command to add console application access if necessary. See the "security login" commands for details.

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 the 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 BlueXP 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
- Deploying a Connector in Azure
- Deploying a Connector on a Linux host
- Switching between Connectors

**Verify that you have the necessary Connector permissions**

If you created the Connector using BlueXP version 3.9.7 or greater, then you’re all set.

If you created the Connector using an earlier version of BlueXP, 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.

If the Azure Blob tiering destination exists as a working environment on the Canvas, you can drag the cluster onto the Azure Blob working environment to initiate the setup wizard.
3. **Define Object Storage Name**: Enter a name for this object storage. It must be unique from any other object storage you may be using with aggregates on this cluster.

4. **Select Provider**: Select **Microsoft Azure** and click **Continue**.

5. Complete the steps on the **Create Object Storage** pages:
   
   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.
Access Tier Life Cycle Management

We’ll move the tiered data through the access tiers that you include in the life cycle. Learn more about Azure Blob storage access tiers.

ACCESS TIER SETUP

<table>
<thead>
<tr>
<th>Hot</th>
<th>Cool</th>
<th>No Time Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move data from Hot to Cool after</td>
<td>45 days</td>
<td></td>
</tr>
<tr>
<td>Keep data in this storage class</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

6. 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.

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 Azure Blob object storage.

**What’s next?**
Be sure to subscribe to the Cloud Tiering service.

You can review information about the active and inactive data on the cluster. Learn more about managing your tiering settings.

You can also create additional object storage in cases where you may want to tier data from certain aggregates on a cluster to different object stores. Or if you plan to use FabricPool Mirroring where your tiered data is replicated to an additional object store. Learn more about managing object stores.

**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 BlueXP, 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 BlueXP 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 BlueXP 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

Required application access parameter

The cluster admin user must have “console” Application access. You can verify this using the ONTAP command `security login show`. "console" should appear in the Application column for the "admin" user. Use the `security login create` command to add console application access if necessary. See the "security login" commands for details.

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 the 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 BlueXP 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
- Deploying 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.

   If the Google Cloud Storage tiering destination exists as a working environment on the Canvas, you can drag the cluster onto the Google Cloud Storage working environment to initiate the setup wizard.

3. Define Object Storage Name: Enter a name for this object storage. It must be unique from any other object storage you may be using with aggregates on this cluster.

4. Select Provider: Select Google Cloud and click Continue.

5. Complete the steps on the Create Object Storage pages:
   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.
We’ll move the tiered data through the storage classes that you include in the life cycle. Learn more about Google Cloud Storage classes.

**Standard**
- Move data from Standard to Nearline after 30 days
- Keep data in this storage class

**Nearline**
- Move data from Nearline to Coldline after 60 days
- Keep data in this storage class

**Coldline**
- Move data from Coldline to Archive after 270 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.

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

7. 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.

8. 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 review information about the active and inactive data on the cluster. Learn more about managing your tiering settings.

You can also create additional object storage in cases where you may want to tier data from certain aggregates on a cluster to different object stores. Or if you plan to use FabricPool Mirroring where your tiered data is replicated to an additional object store. Learn more about managing object stores.

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 BlueXP, 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:

![Diagram showing tiering setup](image)

- 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

**Required application access parameter**

The cluster admin user must have “console” Application access. You can verify this using the ONTAP command `security login show`. "console" should appear in the **Application** column for the "admin" user. Use the `security login create` command to add console application access if necessary. See the "security login" commands for details.
Licensing

A Cloud Tiering license isn’t required in your BlueXP 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 the 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 BlueXP 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:
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
- Deploying a 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.

   If the StorageGRID tiering destination exists as a working environment on the Canvas, you can drag the cluster onto the StorageGRID working environment to initiate the setup wizard.
3. **Define Object Storage Name**: Enter a name for this object storage. It must be unique from any other object storage you may be using with aggregates on this cluster.

4. **Select Provider**: Select **StorageGRID** and click **Continue**.

5. Complete the steps on the **Create Object Storage** pages:
   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.

6. 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.

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 StorageGRID.

What’s next?
You can review information about the active and inactive data on the cluster. Learn more about managing your tiering settings.

You can also create additional object storage in cases where you may want to tier data from certain aggregates on a cluster to different object stores. Or if you plan to use FabricPool Mirroring where your tiered data is replicated to an additional object store. Learn more about managing object stores.

**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.

![Warning icon](https://i.imgur.com/12345.png)

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 BlueXP, 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 BlueXP 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 BlueXP 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

Required application access parameter

The cluster admin user must have “console" Application access. You can verify this using the ONTAP command `security login show`. "console" should appear in the Application column for the "admin" user. Use the `security login create` command to add console application access if necessary. See the "security login" commands for details.

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 the 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 BlueXP 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
- Deploying a 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. **Define Object Storage Name:** Enter a name for this object storage. It must be unique from any other object storage you may be using with aggregates on this cluster.

4. **Select Provider:** Select **S3 Compatible** and click **Continue**.

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

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

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

7. On the **Tier Volumes** page, select the volumes that you want to configure tiering for and click **Continue**:
   a. To select all volumes, check the box in the title row (✓ *Volume Name*) and click **Configure volumes**.
   b. To select multiple volumes, check the box for each volume (✓ *Volume*1) and click **Configure volumes**.
   c. To select a single volume, click the row (or ✍ icon) for the volume.
8. 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 review information about the active and inactive data on the cluster. Learn more about managing your tiering settings.

You can also create additional object storage in cases where you may want to tier data from certain aggregates on a cluster to different object stores. Or if you plan to use FabricPool Mirroring where your tiered data is replicated to an additional object store. Learn more about managing object stores.

Set up licensing for Cloud Tiering

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

A few notes before you read any further:

• If you’ve already subscribed to the BlueXP subscription (PAYGO) in your cloud provider’s marketplace, then you’re automatically subscribed to Cloud Tiering from on-premises ONTAP systems as well. You’ll see an active subscription in the Cloud Tiering Licensing tab. You won’t need to subscribe again.

• The BYOL Cloud Tiering license is a floating license that you can use across multiple on-premises ONTAP clusters in your BlueXP account. This is different than in the past where you purchased a FabricPool license for each cluster.

• There are no charges when tiering data to StorageGRID, so neither a BYOL license or PAYGO registration is required. This tiered data doesn’t count against the capacity purchased in your license.

Learn more about how licensing works for Cloud Tiering.

Use a Cloud Tiering PAYGO subscription

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

Subscribing from the AWS Marketplace

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

Steps
1. In BlueXP, click Mobility > Tiering > Licensing.
2. Click Subscribe under AWS Marketplace and then click Continue.
3. Subscribe from the AWS Marketplace, and then log back into the BlueXP website to complete the registration.

The following video shows the process:

Subscribing from the Azure Marketplace

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

Steps
1. In BlueXP, click Mobility > Tiering > Licensing.
2. Click Subscribe under Azure Marketplace and then click Continue.
3. Subscribe from the Azure Marketplace, and then log back into the BlueXP website to complete the registration.

The following video shows the process:
Subscribing from the GCP Marketplace

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

Steps

1. In BlueXP, click Mobility > Tiering > Licensing.
2. Click Subscribe under GCP Marketplace and then click Continue.
3. Subscribe from the GCP Marketplace, and then log back into the BlueXP website to complete the registration.

The following video shows the process:


Use an annual contract

Pay for Cloud Tiering annually by purchasing an annual contract.

When tiering inactive data to AWS, you can subscribe to an annual contract available from the AWS Marketplace page. It’s available in 1-, 2-, or 3-year terms.

If you want to use this option, set up your subscription from the Marketplace page and then associate the subscription with your AWS credentials.

Annual contracts are not currently supported when tiering to Azure or GCP.

Use a Cloud Tiering BYOL license

Bring-your-own licenses from NetApp provide 1-, 2-, or 3-year terms. The BYOL Cloud Tiering license is a floating license that you can use across multiple on-premises ONTAP clusters in your BlueXP account. The total tiering capacity defined in your Cloud Tiering license is shared among all of your on-prem clusters, making initial licensing and renewal easy.

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

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

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

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

New Cloud Tiering BYOL licensing starting August 21, 2021

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

The **FabricPool** license that you may have used in the past to tier on-premises ONTAP data to the cloud is being retained only for ONTAP deployments in sites that have no internet access (also known as “dark sites”), and for tiering configurations to IBM Cloud Object Storage. If you’re using this type of configuration, you’ll install a FabricPool license on each cluster using System Manager or the ONTAP CLI.

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

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

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

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

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

**Obtain your Cloud Tiering license file**

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

**Steps**

1. Sign in to the [NetApp Support Site](https://support.netapp.com) and click **Systems > Software Licenses**.
2. Enter your Cloud Tiering license serial number.
3. Under License Key, click Get NetApp License File.

4. Enter your BlueXP Account ID (this is called a Tenant ID on the support site) and click Submit to download the license file.

Add Cloud Tiering BYOL licenses to your account

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

Steps

1. Click All Services > Digital Wallet > Data Services Licenses.

2. Click Add License.

3. In the Add License dialog, enter the license information and click Add License:
   - If you have the tiering license serial number and know your NSS account, select the Enter Serial Number option and enter that information.
     
     If your NetApp Support Site account isn’t available from the drop-down list, add the NSS account to BlueXP.
     
     If you have the tiering license file, select the Upload License File option and follow the prompts to attach the file.
Result
BlueXP adds the license so that your Cloud Tiering service is active.

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

This status also appears in the Digital Wallet page.

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

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

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

2. If BlueXP can’t automatically update the license, then you’ll need to manually upload the license file.
   a. You can obtain the license file from the NetApp Support Site.
   b. On the Digital Wallet page in the Data Services Licenses tab, click for the service serial number you are updating, and click Update License.
   c. In the Update License page, upload the license file and click Update License.

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

Apply Cloud Tiering licenses to clusters in special configurations

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

• Clusters that are tiered to IBM Cloud Object Storage
• Cluster that are installed in "dark sites"

Process for existing clusters that have a FabricPool license

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

Process for newly created clusters

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

1. The "parent" Cloud Tiering license tracks the capacity being used for tiering by all clusters to make sure there is enough capacity in the license. The total licensed capacity and expiration date are shown in the Digital Wallet.
2. A "child" tiering license is automatically installed on each cluster to communicate with the "parent" license.
The licensed capacity and expiration date shown in System Manager or in the ONTAP CLI for the "child" license is not the real information, so don’t be concerned if the information is not the same. These values are managed internally by the Cloud Tiering software. The real information is tracked in the Digital Wallet.

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

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

**Steps**

1. Install and configure your ONTAP clusters using System Manager or the ONTAP CLI.
   
   Do not configure tiering at this point.

2. **Purchase a Cloud Tiering license** for the capacity needed for the new cluster, or clusters.

3. In BlueXP, **add the license to the Digital Wallet**.

4. In Cloud Tiering, **discover the new clusters**.

5. From the Cluster Dashboard, click *** for the cluster and select **Deploy License**.

6. In the **Deploy License** dialog, click **Deploy**.
   
   The child license is deployed to the ONTAP cluster.

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

   **FabricPool Mirror configuration information**

   **FabricPool MetroCluster configuration information**

   **Tiering to IBM Cloud Object Storage information**

**Cloud Tiering technical FAQ**

This FAQ can help if you’re just looking for a quick answer to a question.
Cloud Tiering service

The following FAQs relate to how Cloud Tiering works.

What are the benefits of using the Cloud Tiering service?

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

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

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

Essentially, any data that is considered inactive on both primary and secondary storage systems is a good target to move to the cloud. On primary systems, such data can include snapshots, historical records, and finished projects. On secondary systems, this includes all volumes that contain copies of primary data made for DR and backup purposes.

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

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

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

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

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

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

What is the difference between FabricPool and Cloud Tiering?

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

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

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

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

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

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

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

How does Cloud Tiering affect the volume capacity?

Cloud Tiering has no effect on the volume’s capacity but rather on the aggregate’s performance tier usage.

Does Cloud Tiering enable Inactive Data Reporting?

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

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

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

Licenses and Costs

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

How much does using Cloud Tiering cost?

When tiering cold data to the public cloud:

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

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

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

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

What happens if I have reached the BYOL capacity limit?

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

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

No, it does not.
Is rehydration of on-prem systems subject to the egress cost charged by the cloud providers?

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

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

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

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

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

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

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

ONTAP

The following questions relate to ONTAP.

Which ONTAP versions does Cloud Tiering support?

Cloud Tiering supports ONTAP version 9.2 and higher.

What types of ONTAP systems are supported?

Cloud Tiering is supported with single-node and high-availability AFF, FAS, and ONTAP Select clusters. Clusters in FabricPool Mirror configurations and MetroCluster configurations are also supported.

Can I tier data from FAS systems with HDDs only?

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

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

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

What about Cloud Volumes ONTAP?

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

What other requirements are necessary for my ONTAP clusters?

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

The following questions relate to object storage.

Which object storage providers are supported?

Cloud Tiering supports the following object storage providers:

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

Can I use my own bucket/container?

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

Which regions are supported?

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

Which S3 storage classes are supported?

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

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

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

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

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

**Which Azure Blob access tiers are supported?**

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

**Which storage classes are supported for Google Cloud Storage?**

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

**Does Cloud Tiering support the use of life cycle management policies?**

Yes. You can enable life cycle management so that Cloud Tiering transitions data from the default storage class/access tier to a more cost-effective tier after a certain number of days. The life cycle rule is applied to all objects in the selected bucket for Amazon S3 and Google Cloud storage, and to all containers in the selected storage account for Azure Blob.

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

In a typical configuration there is one object store for the entire cluster. Starting in August 2022, you can use the *Advanced Setup* page to add additional object stores for a cluster, and then attach different object stores to different aggregates, or attach 2 object stores to an aggregate for mirroring.

**Can multiple buckets be attached to the same aggregate?**

It is possible to attach up to two buckets per aggregate for the purpose of mirroring, where cold data is synchronously tiered to both buckets. The buckets can be from different providers and different locations. Starting in August 2022, you can use the *Advanced Setup* page to attach two object stores to a single aggregate.

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

Yes. The general best practice is to attach a single bucket to multiple aggregates. However, when using the public cloud there is a maximum IOPS limitation for the object storage services, therefore multiple buckets must be considered.

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

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

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

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

Starting with ONTAP 9.6, if the destination aggregate is using the same cloud tier as the source aggregate, the cold data does not move back to the local tier.
How can I bring my tiered data back on-prem to the performance tier?

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

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

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

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

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

Connectors

The following questions relate to the BlueXP Connector.

What is the Connector?

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

Where does the Connector need to be installed?

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

Can I deploy the Connector on-premises?

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

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

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

What are the implications if the Connector fails?

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

What are the available tiering policies?

There are four tiering policies:

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

Learn more about Tiering Policies.

At which point is my data considered cold?

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

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

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

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

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

Can you choose a tiering size per volume?

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

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

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

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

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

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

Yes. The behavior after the change depends on the new associated policy.
What should I do if I want to ensure certain data is not moved to the cloud?

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

Where is the metadata of the files stored?

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

Networking and security

The following questions relate to networking and security.

What are the networking requirements?

- The ONTAP cluster initiates an HTTPS connection over port 443 to your object storage provider. ONTAP reads and writes data to and from object storage. The object storage never initiates, it just responds.

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

- A Connector needs an outbound HTTPS connection over port 443 to your ONTAP clusters, to the object store, and to the Cloud Tiering service.

For more details, see:

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

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

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

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

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

Is there a network bandwidth recommendation?

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

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

How is my data secured?

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

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

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

What permissions are required?

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

Managing data tiering from your clusters

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

Tiering data from additional volumes

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

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 any additional volumes to the same object store.

Steps

1. From the left navigation menu, select Mobility > Tiering.
2. From the Clusters Dashboard, click Basic Tiering Setup for the cluster.
3. 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.
4. 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.
The selected volumes start to have their data tiered to the cloud.

**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—it does not retroactively move data to the cloud tier.

**Steps**

1. From the left navigation menu, select **Mobility > Tiering**.
2. From the **Clusters Dashboard**, click **Tier Volumes** for the cluster.
3. Click the row for a volume, select a tiering policy, optionally adjust the cooling days, and click **Apply**.

   Learn more about volume tiering policies and cooling days.
**Note:** If you see options to "Retrieve Tiered Data", see *Migrating data from the cloud tier back to the performance tier* for details.

**Result**
The tiering policy is changed and data begins to be tiered based on the new policy.

**Migrating data from the cloud tier back to the performance tier**
Tiered data that is accessed from the cloud may be "re-heated" and moved back to the performance tier. However, if you want to proactively promote data to the performance tier from the cloud tier, you can do this in the *Tiering Policy* dialog. This capability is available when using ONTAP 9.8 and greater.

You might do this if you want to stop using tiering on a volume, or if you decide to keep all user data on the performance tier, but keep Snapshot copies on the cloud tier.

There are two options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Affect on Tiering Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bring back all data</td>
<td>Retrieves all volume data and Snapshot copies tiered in the cloud and promotes them to the performance tier.</td>
<td>Tiering policy is changed to &quot;No policy&quot;.</td>
</tr>
<tr>
<td>Bring back active file system</td>
<td>Retrieves only active file system data tiered in the cloud and promotes it to the performance tier (Snapshot copies remain in the cloud).</td>
<td>Tiering policy is changed to &quot;Cold snapshots&quot;.</td>
</tr>
</tbody>
</table>

You may be charged by your cloud provider based on that amount of data transferred off the cloud.

**Steps**
Make sure you have enough space in the performance tier for all the data that is being moved from the cloud.

1. From the left navigation menu, select *Mobility > Tiering*.
2. From the *Clusters Dashboard*, click *Tier Volumes* for the cluster.
3. Click the **edit** icon for the volume, choose the retrieval option you want to use, and click **Apply**.
Result
The tiering policy is changed and the tiered data starts to be migrated back to the performance tier. Depending on the amount of data in the cloud, the transfer process could take some time.

Managing tiering settings on aggregates

Each aggregate in your on-prem ONTAP systems has two settings that you can adjust: the tiering fullness threshold and whether inactive data reporting is enabled.

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

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

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

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

Steps
1. From the Clusters Dashboard, click Advanced Setup for the selected cluster.
2. From the Advanced Setup page, click the menu icon for the aggregate and select **Modify Aggregate**.

3. In the dialog that is displayed, modify the fullness threshold and choose whether to enable or disable inactive data reporting.

4. Click **Apply**.

**Reviewing tiering info for a cluster**

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

**Steps**
1. From the left navigation menu, select **Mobility > Tiering**.
2. From the **Clusters Dashboard**, click the menu icon for a cluster and select **Cluster info**.
3. Review details about the cluster.

Here's an example:

![Cluster Dashboard Example](image)

You can also view tiering information for a cluster from Digital Advisor if you’re familiar with this NetApp product. Just select **Cloud Recommendations** from the left navigation pane.

![FabricPool Advisor](image)

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

   [A screenshot that shows a Failed tiering health status for a cluster.]

2. Hover over the [A screenshot of the i icon that shows the failure reason] 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 BlueXP has outbound connections to the Cloud Tiering service, to the object store, and to the ONTAP clusters that it discovers.

Discovering additional clusters from Cloud Tiering

You can add your undiscovered on-prem ONTAP clusters to BlueXP from the Tiering Cluster Dashboard so that you can enable tiering for the cluster.

Note that buttons also appear on the Tiering On-Prem Overview page for you to discover additional clusters.

Steps
1. From Cloud Tiering, click the Clusters Dashboard tab.
2. To see any undiscovered clusters, click Show Undiscovered Clusters.

If your NSS credentials are saved in BlueXP, the clusters in your account are displayed in the list.

If your NSS credentials are not saved in BlueXP, you are first prompted to add your credentials before you can see the undiscovered clusters.

3. Scroll down the page to locate the clusters.
4. Click Discover Cluster for the cluster that you want to manage through BlueXP and implement data tiering.

5. On the Choose a Location page On-Premises ONTAP is pre-selected, so just click Continue.

6. On the ONTAP Cluster Details page, enter the password for the admin user account and click Add.

   Note that the cluster management IP address is populated based on information from your NSS account.

7. On the Details & Credentials page the cluster name is added as the Working Environment Name, so just click Go.

Result
BlueXP discovers the cluster and adds it to a working environment in the Canvas using the cluster name as the working environment name.

You can enable the Tiering service or other services for this cluster in the right panel.

Managing object storage used for data tiering

After you've configured your on-prem ONTAP clusters to tier data to a particular object storage, you can perform additional object storage tasks. You can add new object storage, mirror your tiered data to a secondary object storage, swap the primary and mirror object storage, remove a mirrored object store from an aggregate, and more.

Viewing object stores configured for a cluster

You might want to see all the object stores that have been configured for your cluster and to which aggregates they are attached. Cloud Tiering provides this information for each cluster.

Steps
1. From the Clusters Dashboard, click the menu icon for a cluster and select Object Store Info.
2. Review details about the object stores.

This example shows both an Amazon S3 and Azure Blob object store attached to different aggregates on a cluster.

Adding a new object store

You can add a new object store that will be available for aggregates in your cluster. After you create it, you can attach it to an aggregate.

Steps

1. From the Clusters Dashboard, click the menu icon for a cluster and select Object Store Info.
2. From the Object Store Information page, click Create New Object Store.

3. Define Object Storage Name: Enter a name for this object storage. It must be unique from any other object storage you may be using with aggregates on this cluster.
4. Select Provider: Select the provider, for example Amazon Web Services, and click Continue.
5. Complete the steps on the Create Object Storage pages:
   a. S3 Bucket: Add a new S3 bucket or select an existing S3 bucket that starts with the prefix fabric-pool. Then enter the AWS Account ID that provides access to the bucket, select the bucket region, and click Continue.
The \textit{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 \textit{fabric-pool-AFF1}, where AFF1 is the name of the cluster.

b. \textbf{Storage Class Life Cycle}: Cloud Tiering manages the life cycle transitions of your tiered data. Data starts in the \textit{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 \textit{Continue}. For example, the screenshot below shows that tiered data is moved from the \textit{Standard} class to the \textit{Standard-IA} class after 45 days in object storage.

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

![Storage Life Cycle Management](image)

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

c. \textbf{Credentials}: Enter the access key ID and secret key for an IAM user who has the required S3 permissions, and click \textit{Continue}.

The IAM user must be in the same AWS account as the bucket that you selected or created on the \textit{S3 Bucket} page. See the required permissions in the section about activating tiering.

d. \textbf{Cluster Network}: Select the IPspace that ONTAP should use to connect to object storage, and click \textit{Continue}.

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

The object store is created.

Now you can attach the object store to an aggregate in your cluster.

**Attaching a second object store to an aggregate for mirroring**

You can attach a second object store to an aggregate to create a FabricPool mirror to synchronously tier data to two object stores. You must have one object store already attached to the aggregate. Learn more about
FabricPool mirrors.

When using a MetroCluster configuration, it’s a best practice to use object stores in the public cloud that are in different availability zones. Learn more about MetroCluster requirements in the ONTAP documentation.

Note that when using StorageGRID as your object store in a MetroCluster configuration, both ONTAP systems can perform FabricPool tiering to a single StorageGRID system. Each ONTAP system must tier data to different buckets.

Steps
1. From the Clusters Dashboard, click Advanced Setup for the selected cluster.

2. From the Advanced Setup page, drag the object store you want to use to the location for the mirror object store.

3. In the Attach Object Store dialog, click Attach and the second object store is attached to the aggregate.
The Mirror status will appear as "Sync in progress" while the 2 object stores are synchronizing. The status will change to "Synchronized" when synchronization is complete.

**Swapping the primary and mirror object store**

You can swap the primary and mirror object store for an aggregate. The object store mirror becomes the primary, and the original primary becomes the mirror.

**Steps**

1. From the **Clusters Dashboard**, click **Advanced Setup** for the selected cluster.

2. From the Advanced Setup page, click the menu icon for the aggregate and select **Swap Destinations**.

3. Approve the action in the dialog box and the primary and mirror objects stores are swapped.
Removing a mirror object store from an aggregate

You can remove a FabricPool mirror if you no longer need to replicate to an additional object store.

Steps
1. From the Clusters Dashboard, click Advanced Setup for the selected cluster.

   ![Clusters Dashboard](image1)

2. From the Advanced Setup page, click the menu icon for the aggregate and select Unmirror Object Store.

   ![Unmirror Object Store](image2)

The mirror object store is removed from the aggregate and the tiered data is no longer replicated.

When removing the mirror object store from a MetroCluster configuration you'll be prompted whether you want to remove the primary object store as well. You can choose to keep the primary object store attached to the aggregate, or to remove it.

Migrating your tiered data to a different cloud provider

Cloud Tiering enables you to easily migrate your tiered data to a different cloud provider. For example, if you want to move from Amazon S3 to Azure Blob, you can follow the steps listed above in this order:

1. Add an Azure Blob object store.
2. Attach this new object store as the mirror to the existing aggregate.
3. Swap the primary and mirror object stores.
4. Unmirror the Amazon S3 object store.
Measure network latency and throughput performance

Run a Cloud Performance Test to measure network latency and throughput performance from an ONTAP cluster to an object store before and after setting up data tiering. The test also identifies any failures that occurred.

Here are sample performance results:

![Your cluster performance results](image)

<table>
<thead>
<tr>
<th>Operation</th>
<th>Size</th>
<th>Avg. Latency (ms)</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUT</td>
<td>4 MB</td>
<td>502</td>
<td>408.06 MB</td>
</tr>
<tr>
<td>GET</td>
<td>4 KB</td>
<td>79</td>
<td>15.05 MB</td>
</tr>
<tr>
<td>GET</td>
<td>8 KB</td>
<td>197</td>
<td>28.35 MB</td>
</tr>
<tr>
<td>GET</td>
<td>32 KB</td>
<td>291</td>
<td>109.71 MB</td>
</tr>
<tr>
<td>GET</td>
<td>256 KB</td>
<td>361</td>
<td>714.39 MB</td>
</tr>
</tbody>
</table>

Before you get started

It's best to run this check when the cluster is under 50% CPU utilization.

Steps for a cluster that hasn’t been set up for tiering

1. From the left navigation menu, select Mobility > Tiering.
2. From the Cluster Dashboard, click the menu icon for a cluster and select Cloud Performance Test.
3. Review the details and click Continue.
4. Follow the prompts to provide the required information.

   The information that you need to provide is the same as if you were setting up tiering on the cluster.
5. Optionally continue to the Tier Volumes wizard to complete the setup.

Steps for a cluster that has been set up for tiering

1. From the left navigation menu, select Mobility > Tiering.
2. From the Cluster Dashboard, click the menu icon for a cluster and select Cloud Performance Test.
3. Select a node from the drop-down list.
4. View the results or recheck the performance.
Get an overview of data tiering from your clusters

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

Just click **Tiering > On-Prem Overview**. Cloud Tiering provides the following details about your environment.

**Active Clusters**
The number of clusters that are currently tiering data to the cloud, the clusters that aren’t tiering data to the cloud, and the number of clusters that don’t support data tiering.

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

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

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

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

Supported S3 storage classes and regions

Cloud Tiering supports several S3 storage classes and most regions.

Supported S3 storage classes

When you set up data tiering to AWS, Cloud Tiering automatically uses the Standard storage class for your inactive data. Cloud Tiering can apply a lifecycle rule so the data transitions from the Standard storage class to another storage class after a certain number of days. You can choose from the following storage classes:

- Standard-Infrequent Access
- One Zone-Infrequent Access
- Intelligent-Tiering (where AWS automatically moves data between two tiers — Frequent Access and Infrequent Access - when access patterns change)
- Glacier Instant Retrieval

If you do not choose another storage class, then the data remains in the Standard storage class and no rules are applied.

When you configure a Cloud Tiering lifecycle rule, you must not configure any lifecycle rules when setting up the bucket in your AWS account.

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
- 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 two access tiers 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. Cloud Tiering can apply a lifecycle rule so the data transitions from the Hot access tier to the Cool access tier after a certain number of days.

If you do not choose the Cool access tier, then the data remains in the Hot access tier and no rules are applied.

When you configure a Cloud Tiering lifecycle rule, you must not configure any lifecycle rules when setting up the container in your Azure account.

Learn about Azure Blob access tiers.

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 West Central
- Germany North
- 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 several Google Cloud storage classes and most regions.

Supported GCP storage classes

When you set up data tiering to GCP, Cloud Tiering automatically uses the Standard storage class for your inactive data. Cloud Tiering can apply a lifecycle rule so the data transitions from the Standard storage class to other storage classes after a certain number of days. You can choose from the following storage classes:

- Nearline
- Coldline
- Archive

If you do not choose another storage class, then the data remains in the Standard storage class and no rules are applied.

When you configure a Cloud Tiering lifecycle rule, you must not configure any lifecycle rules when setting up the bucket in your Google account.
Learn about Google Cloud Storage classes.

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
Knowledge and support

Register for support

Before you can open a support case with NetApp technical support, you need to add a NetApp Support Site (NSS) account to BlueXP and then register for support.

Support registration overview

There are two forms of registration to activate support entitlement:

• Registering your BlueXP account ID support subscription (your 20 digit 960xxxxxxxxx serial number located on the Support Resources page in BlueXP).

  This serves as your single support subscription ID for any service within BlueXP. Each BlueXP account-level support subscription must be registered.

• Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider’s marketplace (these are 20 digit 909201xxxxxxxx serial numbers).

  These serial numbers are commonly referred to as PAYGO serial numbers and get generated by BlueXP at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets and automatic case generation.

How you register depends on whether you’re a new or existing customer or partner.

• Existing customer or partner

  As an existing NetApp customer or partner, you can use your NetApp Support Site (NSS) SSO account to perform these registrations above. In the Support Dashboard, BlueXP provides an NSS Management page where you can add your NSS account. Once you add your NSS account, BlueXP automatically registers these serial numbers for you.

  Learn how to add your NSS account.

• New to NetApp

  If you’re brand new to NetApp, you must complete a one-time registration of your BlueXP account ID serial number on NetApp’s support registration site. Once you complete this registration and create a new NSS account, you can use this account in BlueXP to auto register going forward.

  Learn how to register with NetApp.

Add an NSS account to BlueXP

The Support Dashboard enables you to add and manage your NetApp Support Site accounts for use with Cloud Manager.

• If you have a customer-level account, you can add one or more NSS accounts.

• If you have a partner or reseller account, you can add one or more NSS accounts, but they can’t be added
alongside customer-level accounts.

**Steps**

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.

![BlueXP console with selected Help and Support options](image)

2. Click **NSS Management > Add NSS Account**.

3. When you’re prompted, click **Continue** to be redirected to a Microsoft login page.

NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

4. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

Note the following:

- The account must be a customer-level account (not a guest or temp account).
- Upon successful login, NetApp will store the NSS user name. This is a system generated ID that maps to your email. On the **NSS Management** page, you can display your email from the *** menu.
- If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the *** menu. Using this option prompts you to log in again.

**Register with NetApp**

How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

**Existing customer with an NSS account**

If you’re a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

**Steps**
1. In the upper right of the BlueXP console, click the Help icon, and select Support.

2. If you haven’t already done so, add your NSS account to BlueXP.

3. On the Resources page, click Register for Support.

Existing customer but no NSS account

If you’re an existing NetApp customer with existing licenses and serial numbers but no NSS account, you just need to create an NSS account.

Steps
1. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically NetApp Customer/End User.
   b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

Brand new to NetApp

If you are brand new to NetApp and you don’t have an NSS account, follow each step below.

Steps
1. In the upper right of the BlueXP console, click the Help icon, and select Support.
2. Locate your Cloud Manager account ID serial number from the Support Registration page.

3. Navigate to NetApp’s support registration site and select I am not a registered NetApp Customer.

4. Fill out the mandatory fields (those with red asterisks).

5. In the Product Line field, select Cloud Manager and then select your applicable billing provider.

6. Copy your Cloud Manager account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

   An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn’t arrive in few minutes.

7. Confirm the action from within the email.

   Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically NetApp Customer/End User.
   b. Be sure to copy the Cloud Manager Account Serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, you can navigate to BlueXP to add this NSS account for future registrations.

Get help

NetApp provides support for BlueXP and its cloud services in a variety of ways. Extensive free self-support
options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

**Self support**

These options are available for free, 24 hours a day, 7 days a week:

- **Knowledge base**
  
  Search through the BlueXP knowledge base to find helpful articles to troubleshoot issues.

- **Communities**
  
  Join the BlueXP community to follow ongoing discussions or create new ones.

- **Documentation**
  
  The BlueXP documentation that you’re currently viewing.

- **Feedback email**
  
  We value your input. Submit feedback to help us improve BlueXP.

**NetApp support**

In addition to the self-support options above, you can work with a NetApp Support specialist to resolve any issues after you activate support.

**Before you get started**

To use the **Create a Case** capability, you must first perform a one-time registration of your BlueXP Account ID serial number (ie. 960xxxx) with NetApp. Learn how to register for support.

**Steps**

1. In BlueXP, click **Help > Support**.

2. Choose one of the available options under Technical Support:
   a. Click **Call Us** if you’d like to speak with someone on the phone. You’ll be directed to a page on netapp.com that lists the phone numbers that you can call.
   b. Click **Create a Case** to open a ticket with a NetApp Support specialists:

      - **NetApp Support Site Account**: Select the applicable NSS account associated with the person opening the support case. This person will be the primary contact for NetApp to reach out to, in addition to the additional emails provided below.

      If you don’t see your NSS account, you can navigate to the **NSS Management** tab within Support section of BlueXP to add it there.

      - **Service**: Select the service that the issue is associated with. For example, BlueXP when specific to a technical support issue with workflows or functionality within the service.

      - **Working Environment**: If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.

      The list of working environments are within scope of the BlueXP account, workspace, and Connector you have selected in the top banner of the service.
- **Case Priority**: Choose the priority for the case, which can be Low, Medium, High, or Critical.

  To learn more details about these priorities, hover your mouse over the information icon next to the field name.

- **Issue Description**: Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

- **Additional Email Addresses**: Enter additional email addresses if you’d like to make someone else aware of this issue.

---

![Create a Case](image)

**After you finish**

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.
For a history of your support cases, you can click **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It’s possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it’s associated with is not the same company of record for the BlueXP account serial number (ie. 960xxxx) or the working environment serial number. You can check your list of NSS accounts at the top of the **Create a Case** form to find the right match, or you can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at [https://mysupport.netapp.com/site/help](https://mysupport.netapp.com/site/help)
Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright


Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.


Patents

A current list of NetApp owned patents can be found at:


Privacy policy


Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- Notice for BlueXP
- Notice for Cloud Tiering
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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a nonexclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.