Cloud Tiering technical FAQ

Cloud Manager

Tom Onacki, Ben Cammett
August 11, 2021

Table of Contents

Cloud Tiering technical FAQ

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

ONTAP

The following questions relate to ONTAP.

What are the requirements for my ONTAP cluster?

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

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

Does Cloud Tiering enable inactive data reporting?

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

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

Can I tier data from NAS volumes and SAN volumes?

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

What about Cloud Volumes ONTAP?

If you have Cloud Volumes ONTAP systems, you'll find them in the Cluster Dashboard so you get a full view of data tiering in your hybrid cloud infrastructure.

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

Cloud Volumes ONTAP systems are read-only from Cloud Tiering. You can't set up data tiering on Cloud Volumes ONTAP from Cloud Tiering. You set up tiering for Cloud Volumes ONTAP from the working environment in Cloud Manager.

Object storage

The following questions relate to object storage.

Which object storage providers are supported?

Amazon S3, Azure Blob storage, Google Cloud Storage, NetApp StorageGRID, and S3-compatible object storage providers are supported.

Can I use my own bucket/container?

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

Which regions are supported?

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

Which S3 storage classes are supported?

Cloud Tiering supports data tiering to the *Standard*, *Standard-Infrequent Access*, *One Zone-IA*, or *Intelligent* storage classes. See Supported S3 storage classes for more details.

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

One object store for the entire cluster.

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

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.

Connectors

The following questions relate to Connectors.

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.

Networking

The following questions relate to networking.

What are the networking requirements?

- The ONTAP cluster initiates an HTTPS connection over port 443 to your object storage provider.

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

- For StorageGRID, the ONTAP cluster initiates an HTTPS connection over a user-specified port to StorageGRID (the port is configurable during tiering setup).
- A Connector needs an outbound HTTPS connection over port 443 to your ONTAP clusters, to the object store, and to the Cloud Tiering service.

For more details, see:

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

Permissions

The following questions relate to permissions.

What permissions are required in AWS?

Permissions are required to manage the S3 bucket.

What permissions are required in Azure?

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

What permissions are required in Google Cloud Platform?

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

What permissions are required for StorageGRID?

S3 permissions are needed.

What permissions are required for S3-compatible object storage?

S3 permissions are needed.