Tier data to Google Cloud Storage

Cloud Tiering

NetApp
March 06, 2021

Table of Contents

Tier data to Google Cloud Storage . . . 1
Quick start for tiering inactive data to Google Cloud Storage . . . 1
Preparing to tier inactive data to Google Cloud Storage . . . 1
Tiering inactive data from your first cluster to Google Cloud Storage . . . 5
Supported Google Cloud storage classes and regions . . . 8

Tier data to Google Cloud Storage

Quick start for tiering inactive data to Google Cloud Storage

Start tiering inactive data to Google Cloud Storage by completing a few steps.

Prepare to tier data to Google Cloud Storage

You need the following:

- An AFF or FAS system with all-SSD aggregates that's running ONTAP 9.6 or later and has an HTTPS connection to Google Cloud Storage.
- A service account that has the predefined Storage Admin role and storage access keys.
- A service account that includes the permissions defined in the Service Connector policy for GCP.
- Google Cloud APIs enabled in your project: Cloud Deployment Manager V2 API, Cloud Resource Manager API, and Compute Engine API.
- A GCP user that has the required permissions to deploy the Service Connector in a Google Cloud Platform VPC.

  The VPC where you deploy the Service Connector must provide an outbound HTTPS connection to the ONTAP cluster in your data center, to Google Cloud Storage, and to the Cloud Tiering service.

For step-by-step instructions, see Preparing to tier inactive data to Google Cloud Storage.

Tier inactive data from your first cluster

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

For step-by-step instructions, see Tiering inactive data from your first cluster to Google Cloud Storage.

Set up licensing

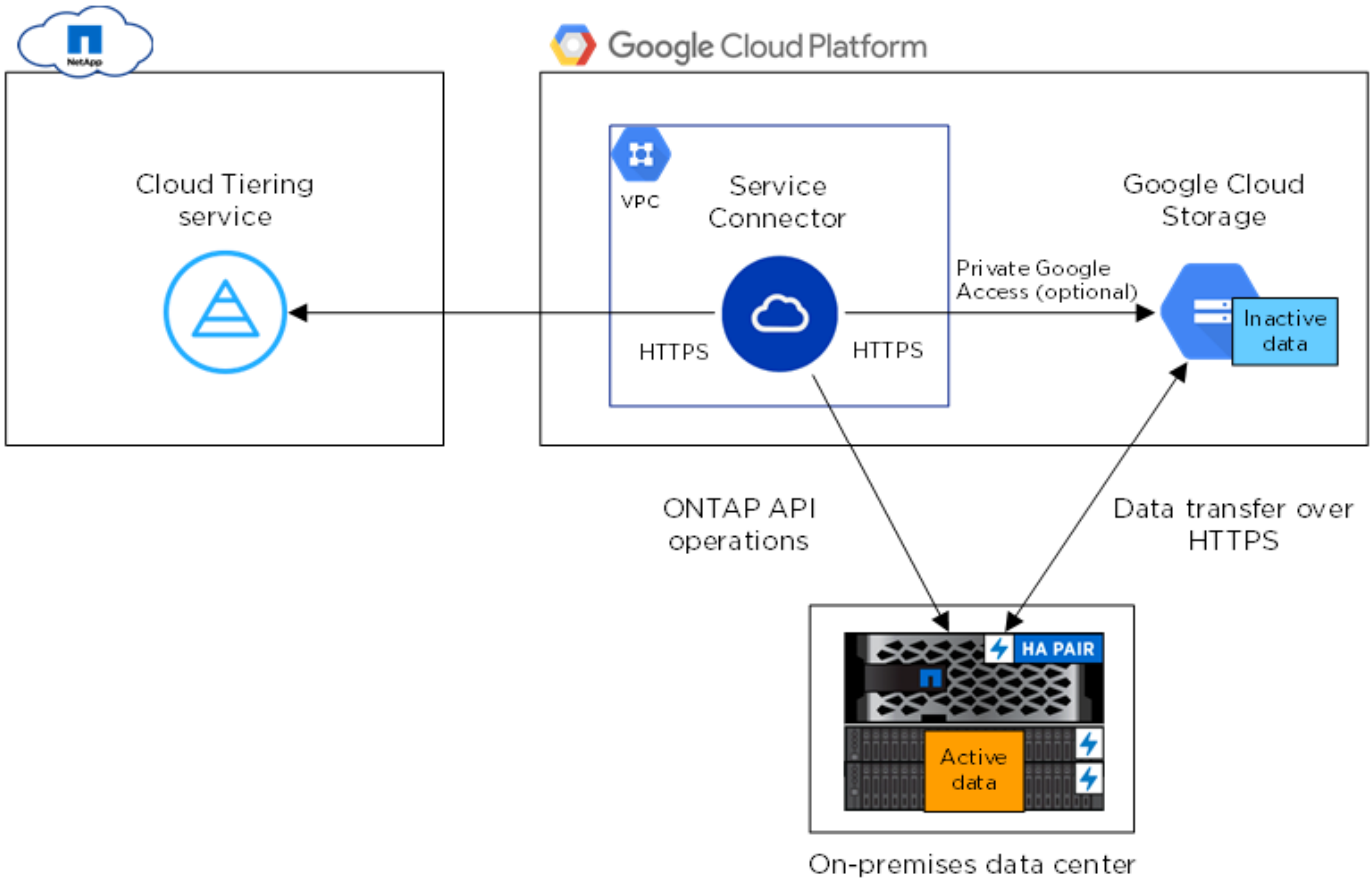
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both:

- To subscribe from the GCP Marketplace, click **Licensing**, click **Subscribe**, and then follow the prompts.
- To add a tiering license, contact us if you need to purchase one, and then add it to your cluster from ONTAP System Manager.

Preparing to tier inactive data to Google Cloud Storage

Before you start tiering data, verify support for your ONTAP cluster, provide the required permissions, and set up your networking.

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



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

Preparing your ONTAP clusters

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

Supported ONTAP platforms

Cloud Tiering supports AFF systems and all-SSD aggregates on FAS systems.

Supported ONTAP versions

ONTAP 9.6 or later

Cluster networking requirements

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

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

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

- An inbound connection is required from the NetApp Service Connector, which resides in an Google

Cloud Platform VPC.

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

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

  IPspaces enable network traffic segregation, allowing for separation of client traffic for privacy and security. Learn more about IPspaces.

  When you set up data tiering, Cloud Tiering prompts you for the IPspace to use. You should choose the IPspace that each LIF is associated with. That might be the "Default" IPspace or a custom IPspace that you created.

Supported volumes and aggregates

The total number of volumes that Cloud Tiering can tier might be less than the number of volumes on your ONTAP system. That's because volumes can't be tiered from some aggregates. For example, you can't tier data from SnapLock volumes or from MetroCluster configurations. Refer to ONTAP documentation for functionality or features not supported by FabricPool.

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

Preparing to deploy the Service Connector in GCP

The Service Connector is NetApp software that communicates with your ONTAP clusters. Cloud Tiering guides you through the process of deploying the Service Connector on a GCP virtual machine instance.

A few steps are required before you can deploy the Service Connector in GCP. You'll need to provide the required permissions, set up a service account, and set up your networking.

It's important to note that Cloud Tiering tiers data to a Google Cloud bucket that resides in the same project as the Service Connector. So be sure to complete these steps in the project where both the Service Connector and bucket should reside.

Steps

1. Set up GCP permissions.
2. Set up a service account.
3. Set up networking.

Setting up GCP permissions

Ensure that your GCP user has the required permissions to deploy the NetApp Service Connector in a Google Cloud Platform VPC. You also need to enable a few APIs in the project.

Steps

1. Ensure that the GCP user who deploys the Service Connector has the permissions in the Cloud Central policy for GCP.

   You can create a custom role using the YAML file and then attach it to the user. You'll need to use the gcloud command line to create the role.

2. Enable the following Google Cloud APIs in your project:

- Cloud Deployment Manager V2 API
- Cloud Resource Manager API
- Compute Engine API

Result

The GCP user now has the permissions required to deploy the Service Connector in GCP from Cloud Tiering.

Setting up a service account

When you deploy the Service Connector from Cloud Tiering, you need to select a service account to associate with the VM instance. This service account needs specific permissions to enable management of tiering.

Steps

1. Create a role in GCP that includes the permissions defined in the Service Connector policy for GCP.

   You'll need to use the gcloud command line to create the role.

2. Create a GCP service account and apply the custom role that you just created.

Setting up GCP networking

Cloud Tiering prompts you for the VPC where the Service Connector should be deployed. Make sure that the VPC provides the required networking connections.

Steps

1. Identify a VPC for the Service Connector that enables the following connections:
   - An outbound internet connection to the Cloud Tiering service over port 443 (HTTPS)
   - An HTTPS connection over port 443 to Google Cloud Storage
   - An HTTPS connection over port 443 to your ONTAP clusters

     Cloud Tiering enables you to deploy the virtual machine with a public IP address and you can configure it to use your own proxy server.

     You don't need to create your own firewall rules for the instance because Cloud Tiering can do that for you. The firewall rules that Cloud Tiering creates allows inbound connectivity over HTTP, HTTPS, and SSH. Outbound connectivity is open.

2. Optional: Enable Private Google Access on the subnet where you plan to deploy the Service Connector.

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

Preparing Google Cloud Storage for data tiering

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

Steps

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

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

Tiering inactive data from your first cluster to Google Cloud Storage

After you prepare your Google Cloud environment, just log in to Cloud Tiering and start tiering inactive data from your first cluster.

What you'll need

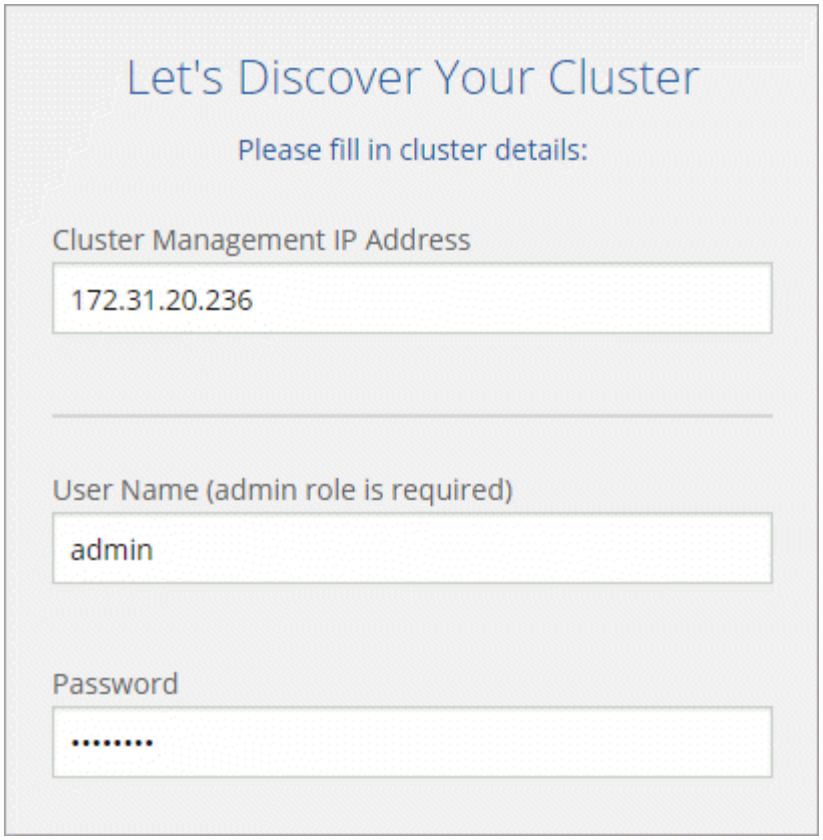
- To discover the cluster, you'll need the following:
  - The cluster management IP address.
  - The user name and password of an ONTAP account that has administrator-level privileges.

    The Service Connector uses this account to send API operations to the ONTAP cluster.
- To deploy the Service Connector in GCP, you'll need the following:
  - A Google account that has the required permissions to deploy the Service Connector virtual machine.
  - The project, region, VPC, and subnet in which the Service Connector will reside.
  - A service account that includes the permissions defined in the Service Connector policy for GCP.
- To set up tiering to Google Cloud Storage, you'll need storage access keys for a service account that has the Storage Admin role.

If you haven't met these requirements, see Preparing to tier data to Google Cloud Storage.

Steps

1. Log in to NetApp Cloud Central.
2. Select the Cloud Tiering service.
3. Click **Let's Start, Discover Your First Cluster**.
4. Complete the steps on the **Discover Cluster** page:
   a. Enter the cluster management IP address and the user name and password of an account that has administrator-level privileges.



b. Click **Discover Cluster**.

   If you already have an existing Service Connector, then Cloud Tiering automatically attempts to use that Service Connector. Cloud Tiering moves on to the next step, if any existing Service Connector has connectivity to the cluster.

c. If Cloud Tiering prompts you to create a Service Connector, click **Create your first Service Connector**.

   If you have an existing Service Connector and Cloud Tiering can't use it, then you'll need to do one of two things:

   - Click **Add Service Connector** to create a new Service Connector.
   - Check the status and connectivity of any existing Service Connectors and then try to discover the cluster again.

d. If you clicked the button to create a Service Connector, follow the prompts to deploy it in GCP:

   - **Select Provider**: Select **Google Cloud Platform** as the target location for the Service Connector.

     When prompted, sign in and accept the permissions request from Google. The form is owned and hosted by Google. Your credentials are not provided to NetApp.

   - **Basic Settings**: Enter a name for the virtual machine, select a project, and then select a service account that includes the permissions defined in the Service Connector policy for GCP.
   - **Location**: Specify networking for the virtual machine—a region, zone, VPC, and subnet, and then choose whether you want to assign a public IP address and specify an HTTP proxy for outbound connectivity.

     Remember, the Service Connector must have a constant connection to the ONTAP cluster and a

constant internet connection to the Cloud Tiering service.

- **Firewall Policy**: Select **Create a new firewall policy** so Cloud Tiering can create the security group, or select an existing firewall policy. Then click **Go**.

  The firewall policy that Cloud Tiering creates allows inbound HTTP, HTTPS, and SSH connectivity. It has open outbound connectivity.

  Leave the page open until the deployment is complete.

e. Back on the Discover Cluster page, select the Service Connector that you just created.

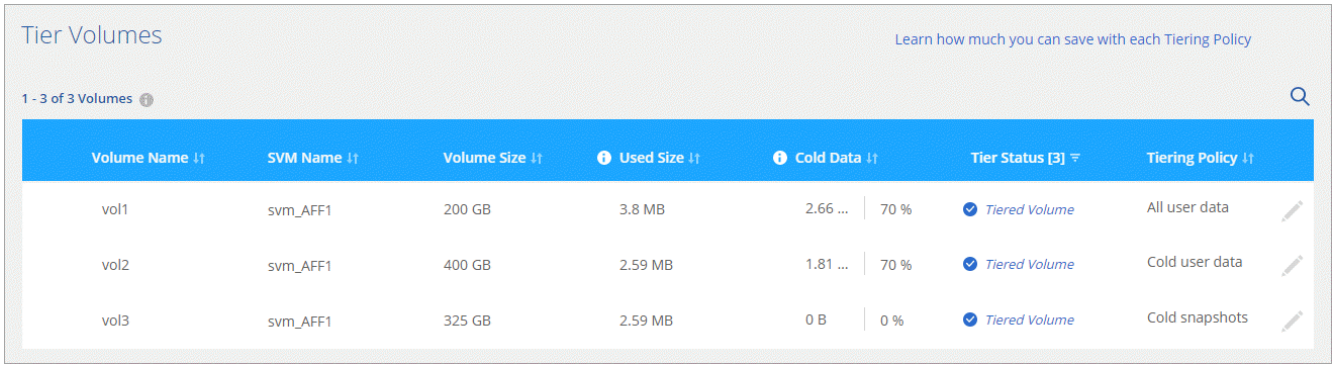
5. Complete the steps on the **Tiering Setup** page:
   a. **Bucket**: Add a new Google Cloud Storage bucket or select an existing bucket and click **Continue**.
   b. **Storage Class**: Select the storage class that you want to use for the tiered data and click **Continue**.
   c. **Credentials**: Enter the storage access key and secret key for a service account that has the Storage Admin role.
   d. **Cluster Network**: Select the IPspace that ONTAP should use to connect to object storage and click **Continue**.

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

      If you haven't reviewed requirements for the IPspace and the associated intercluster LIFs, see ONTAP cluster requirements.

6. Click **Continue** to select the volumes that you want to tier.
7. For each volume, click the icon, select a tiering policy, optionally adjust the cooling days, and click **Apply**.

   Learn about volume tiering policies and cooling days.



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

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 from the GCP Marketplace.

You can also add additional clusters or review information about the active and inactive data on the cluster. For

details, see Managing data tiering from your clusters.

Supported Google Cloud storage classes and regions

Cloud Tiering supports the Standard storage class and most Google Cloud regions.

Supported access tiers

Cloud Tiering uses the *Standard* access tier for your inactive data.

Supported Google Cloud regions

Cloud Tiering supports the following regions.

Americas

- Iowa
- Los Angeles
- Montreal
- N. Virginia
- Oregon
- Sao-Paulo
- South Carolina

Asia Pacific

- Hong Kong
- Mumbai
- Osaka
- Singapore
- Sydney
- Taiwan
- Tokyo

Europe

- Belgium
- Finland
- Frankfurt
- London
- Netherlands
- Zurich