Tier data to Azure Blob storage

Cloud Tiering

NetApp
March 06, 2021

Table of Contents

Tier data to Azure Blob storage

Quick start for tiering inactive data to Azure

Getting started with Cloud Tiering in Microsoft Azure includes a few steps.

Prepare to tier data to Azure Blob storage

You need the following:

- An AFF or FAS system with all-SSD aggregates running ONTAP 9.4 or later, and an HTTPS connection to Azure Blob storage.
- An Azure account that has the required permissions to deploy the Service Connector in a VNet.

  The Service Connector needs an outbound HTTPS connection to the ONTAP cluster in your data center, to Azure Blob storage, and to the Cloud Tiering service.

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**.

Set up licensing

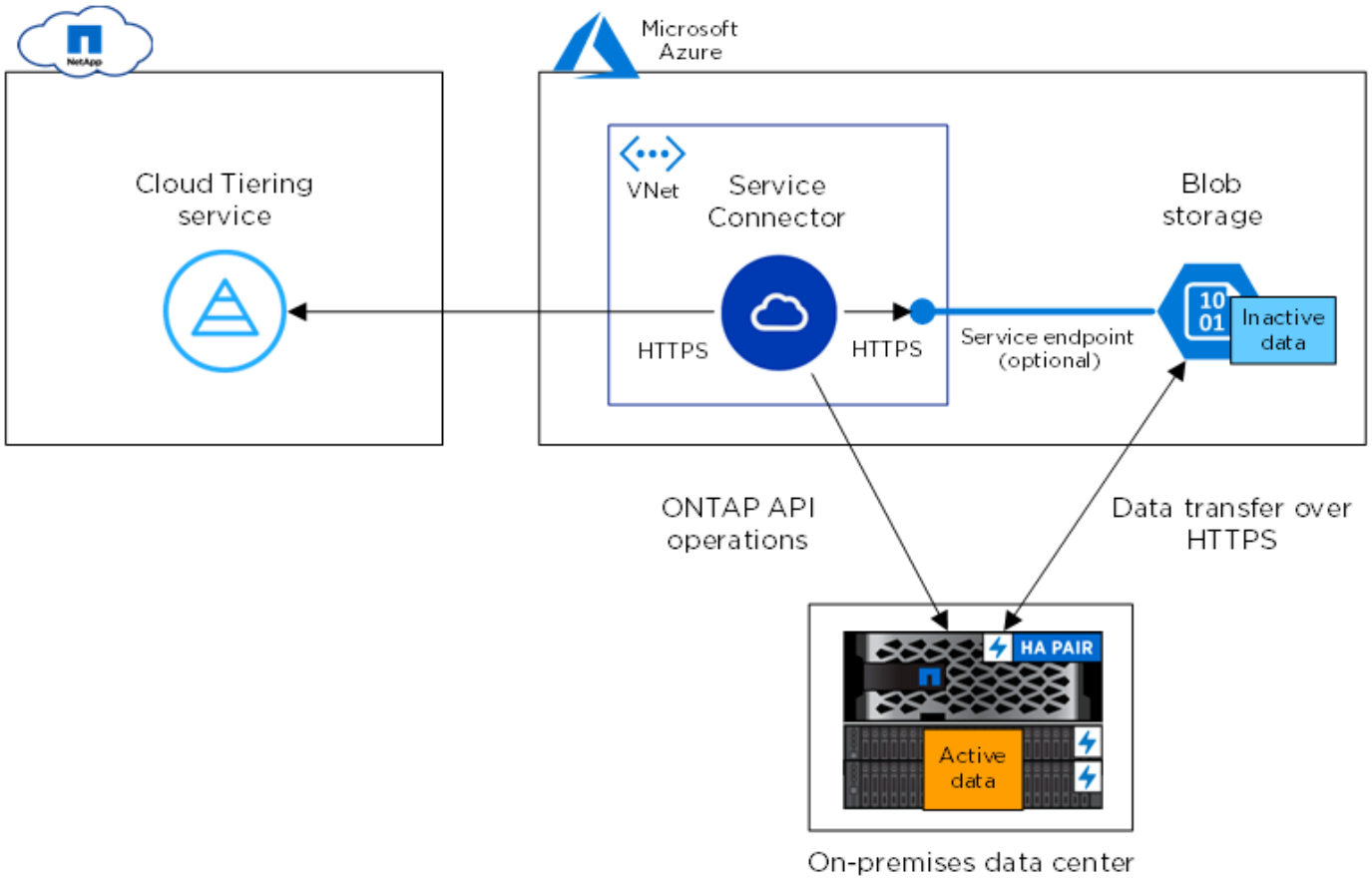
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both:

- To subscribe from the Azure 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 Azure Blob storage

Before you use Cloud Tiering, 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 Blob storage is for object storage setup only.

Preparing your ONTAP clusters

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

Supported ONTAP platforms

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

Supported ONTAP version

ONTAP 9.4 or later

Cluster networking requirements

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

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

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

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

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

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

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

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

Supported volumes and aggregates

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

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

Preparing to deploy the Service Connector in Azure

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 an Azure virtual machine.

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

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

Steps

1. Grant Azure permissions.
2. Set up networking.

Granting Azure permissions

Ensure that your Azure account has the required permissions to deploy the NetApp Service Connector in an Azure VNet.

During deployment, Cloud Tiering creates and assigns a role to the Service Connector that provides the required permissions so ONTAP can tier inactive data to Azure Blob storage.

Steps

1. Create a custom role using the NetApp Cloud Central policy:
   a. Download the Cloud Central policy for Azure.

   Right-click the link and click **Save link as…** to download the file.

   b. Modify the JSON file by adding your Azure subscription ID to the assignable scope.

Example

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
],
```

c. Use the JSON file to create a custom role in Azure.

The following example shows how to create a custom role using the Azure CLI 2.0:

az role definition create --role-definition C:\Policy_for_Setup_As_Service_Azure.json

You should now have a custom role called *Azure SetupAsService*.

2. Assign the role to the user who will deploy the Service Connector from Cloud Tiering:
   a. Open the **Subscriptions** service and select the user's subscription.
   b. Click **Access control (IAM)**.
   c. Click **Add** > **Add role assignment** and then add the permissions:
      - Select the **Azure SetupAsService** role.

        Azure SetupAsService is the default name provided in the Cloud Central policy. If you chose a different name for the role, then select that name instead.

      - Assign access to an **Azure AD user, group, or application**.
      - Select the user account.
      - Click **Save**.

Result

The Azure user now has the permissions required to deploy the Service Connector.

Setting up Azure networking

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

Steps

1. Identify a VNet 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 Azure Blob 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 network security group because Cloud Tiering can do that for you. The security group that Cloud Tiering creates has no inbound connectivity and open outbound connectivity.

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 Service Connector and Blob storage to stay in your virtual private network.

Tiering inactive data from your first cluster to Azure Blob storage

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

What you'll need

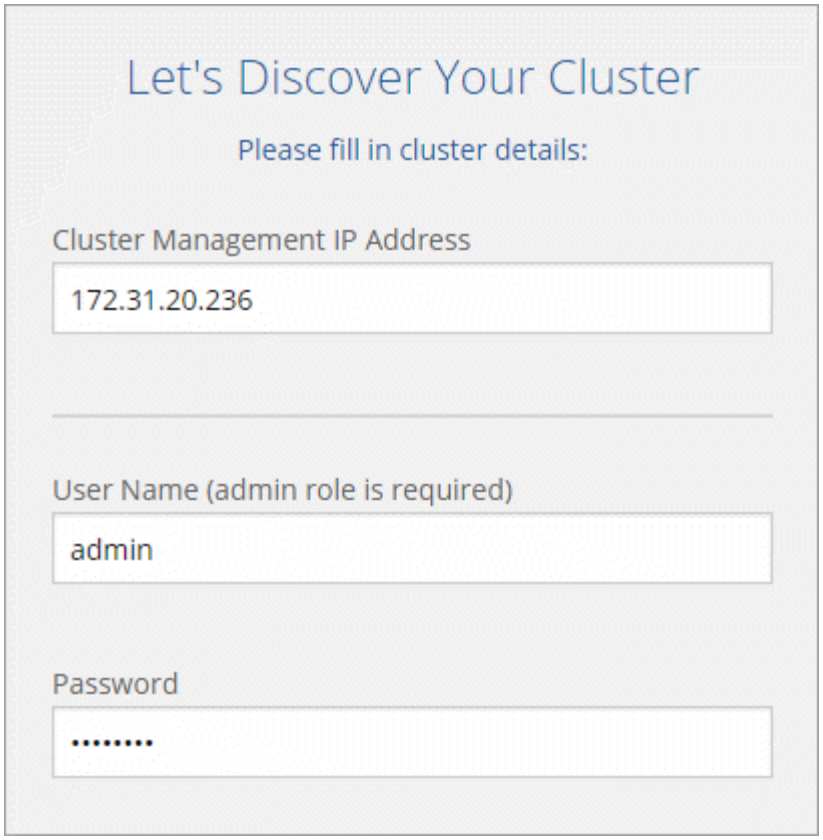
- To discover the cluster, you'll need the following:
  - The cluster management IP address.
  - The user name and password of an ONTAP account that has administrator-level privileges.

    The Service Connector uses this account to send API operations to the ONTAP cluster.
- To deploy the Service Connector in Azure, you'll need the following:
  - An Azure account that has the required permissions to deploy the Service Connector virtual machine.
  - The Azure subscription, region, VNet, and subnet in which the Service Connector will reside.

If you haven't met these requirements, see Preparing to tier data to Azure.

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 Azure:

   - **Select Provider**: Select **Microsoft Azure** as the target location for the Service Connector.

     When prompted, sign in and accept the permissions request from Microsoft.

     The form is owned and hosted by Microsoft. Your credentials are not provided to NetApp.

   - **Virtual Machine Authentication**: Enter a name for the virtual machine and choose an authentication method.
   - **Basic Settings**: Select an Azure subscription, choose a region, and specify a new or existing resource group for the virtual machine.
   - **Network**: Select a VNet and subnet, choose whether to assign a public IP address, and specify an

HTTP proxy, if one is required 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.

- **Security Group**: Select **Create a new security group** so Cloud Tiering can create the security group, or select your own. Then click **Go**.

  The security group that Cloud Tiering creates has no inbound connectivity and 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. **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.

   b. **Azure Container**: Add a new Blob container to a storage account or select an existing container and click **Continue**.

      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**: Select the access tier that you want to use for the tiered data and click **Continue**.

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

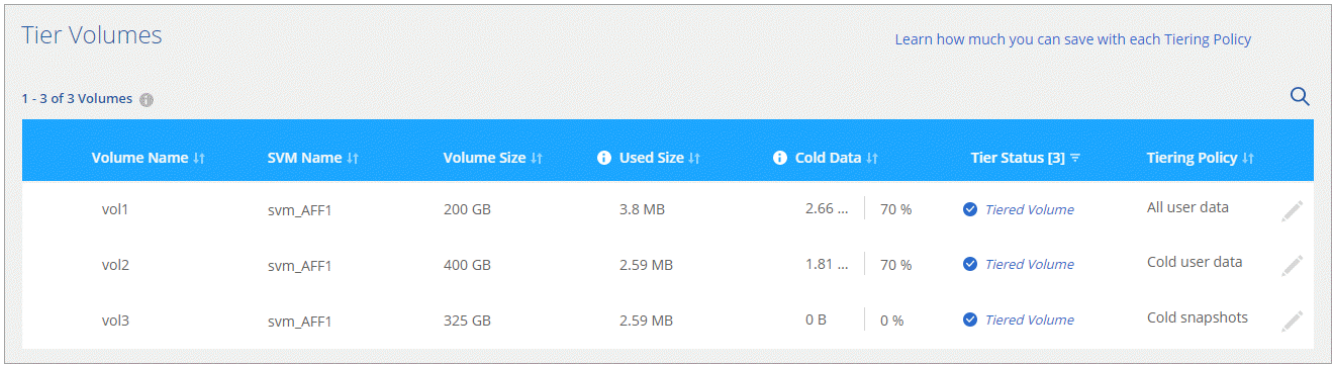
      Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your cloud provider's object storage.

      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 Azure Blob object storage.

What's next?

Be sure to subscribe to the Cloud Tiering service from the Azure 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 Azure Blob access tiers and regions

Cloud Tiering supports the *Hot* access tier and most regions.

Supported Azure Blob access tiers

When you set up data tiering to Azure, Cloud Tiering automatically uses the *Hot* access tier for your inactive data.

Supported Azure regions

Cloud Tiering supports the following Azure regions.

Africa

- South Africa North

Asia Pacific

- Australia East
- Australia Southeast
- East Asia
- Japan East
- Japan West
- Korea Central
- Korea South
- Southeast Asia

Europe

- France Central
- Germany Central
- Germany Northeast
- North Europe
- UK South
- UK West
- West Europe

North America

- Canada Central
- Canada East
- Central US
- East US
- East US 2
- North Central US
- South Central US
- West US
- West US 2
- West Central US

South America

- Brazil South