Tier data to AWS S3

Cloud Tiering

NetApp
September 23, 2021

Table of Contents

Tier data to AWS S3

Quick start for tiering inactive data to AWS

Getting started with Cloud Tiering in AWS includes a few steps.

Prepare to tier data to AWS

You need the following:

- An AFF or FAS system with all-SSD aggregates running ONTAP 9.2 or later, and an HTTPS connection to AWS S3.
- An AWS account that has an access key and the required permissions so the ONTAP cluster can tier inactive data in and out of AWS S3.
- A location for the Service Connector: either an AWS VPC or an on-premises Linux host.

  With either option, the Service Connector needs an outbound HTTPS connection to the ONTAP cluster, to S3 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

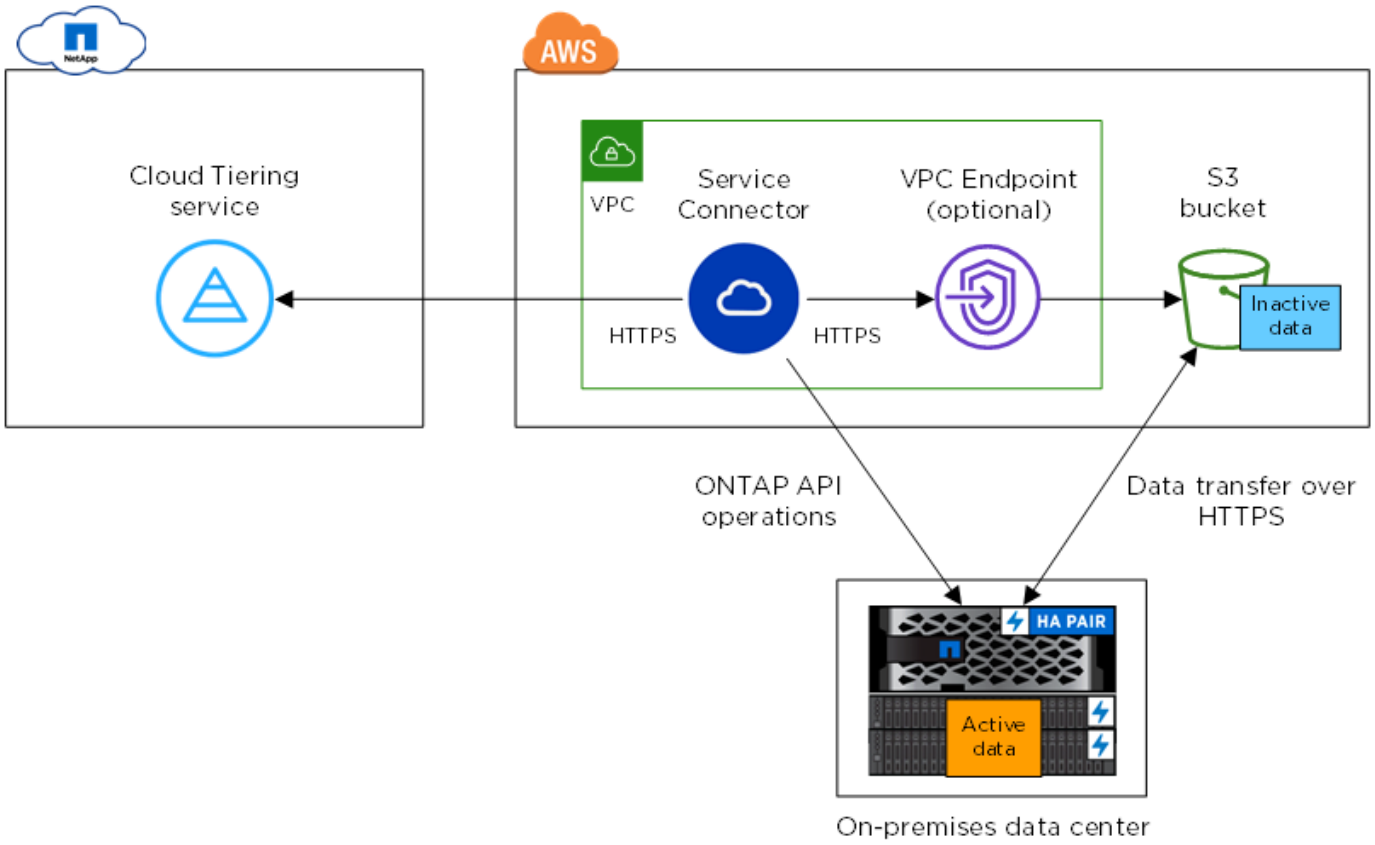
After your free trial ends, pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both:

- To subscribe from the AWS 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 AWS S3

Before you use Cloud Tiering, verify support for your ONTAP cluster, prepare your object storage, and set up a location for the Service Connector.

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



Communication between the Service Connector and S3 is for object storage setup only. The Service 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 AWS S3.

Supported ONTAP platforms

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

Supported ONTAP version

ONTAP 9.2 or later

Cluster networking requirements

- The ONTAP cluster initiates an HTTPS connection over port 443 to AWS S3.

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

  Although AWS Direct Connect provides better performance and lower data transfer charges, it is not required between the ONTAP cluster and AWS S3. Because performance is significantly better when using AWS Direct Connect, doing so is the recommended best practice.

- An inbound connection is required from the NetApp Service Connector, which can reside in an AWS VPC or on your premises.

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

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

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

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

Supported volumes and aggregates

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

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

Choosing a location for the Service Connector

The Service Connector is NetApp software that communicates with your ONTAP clusters. You can deploy the Service Connector on your premises or in an AWS VPC.

Be sure to set up the Service Connector in the same AWS account to which you want to tier data.

- Installing the Service Connector on prem
- Preparing to deploy the Service Connector in an AWS VPC

Preparing to deploy the Service Connector in an AWS VPC

Cloud Tiering guides you through the process of deploying the Service Connector on an EC2 instance. Make sure that your AWS account and networking are set up.

Setting up an AWS account for the Service Connector

The AWS account where you deploy the EC2 instance must have permissions and an access key. Cloud Tiering tiers data to an S3 bucket that resides in the same AWS account as the Service Connector.

Steps

1. Provide the permissions in this policy to the IAM user.

   AWS Documentation: Creating a Role to Delegate Permissions to an IAM User

2. Create or locate an access key that you can provide to Cloud Tiering.

   These credentials are used by the Cloud Tiering service to launch the EC2 instance in AWS. Providing your keys is secure and private. NetApp does not save them.

   AWS Documentation: Managing Access Keys for IAM Users

Setting up AWS networking for the Service Connector

The Service Connector needs a connection to your ONTAP clusters, to AWS S3, and to the Cloud Tiering service.

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 S3
   - An HTTPS connection over port 443 to your ONTAP clusters

     Cloud Tiering enables you to deploy the EC2 instance with a public IP address and you can configure it to use your own proxy server.

     You don't need to create your own 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 VPC Endpoint to S3.

   A VPC Endpoint to S3 is recommended if you have a Direct Connect or VPN connection from your ONTAP cluster to the VPC and you want communication between the Service Connector and S3 to stay in your AWS internal network.

Preparing AWS S3 for data tiering

When you set up data tiering to a new cluster, Cloud Tiering prompts you to create an S3 bucket or select an existing S3 bucket in the AWS account where you set up the Service Connector.

The AWS account must have permissions and an access key that you can enter in Cloud Tiering. The ONTAP cluster uses the access key to tier data in and out of S3.

Steps

1. Provide the following permissions to the IAM user:

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

   AWS Documentation: Creating a Role to Delegate Permissions to an IAM User
2. Create or locate an access key.

   Cloud Tiering passes the access key on to the ONTAP cluster. The credentials are not stored in the Cloud Tiering service.

   AWS Documentation: Managing Access Keys for IAM Users

Installing the Service Connector on your premises for tiering to AWS S3

If you want to tier cold data to AWS S3, you can deploy the Service Connector either on your premises or in an AWS VPC. This page describes how to install the on-premises Service Connector.

To deploy the Service Connector in AWS, follow the prompts in Cloud Tiering when discovering your first cluster.

Understanding the relationship between the Service Connector and Cloud Manager

To install the Service Connector, you need to download and install NetApp Cloud Manager software. You need to do this because the Service Connector is part of Cloud Manager.

Verifying host requirements

Refer to Connector host requirements in the Cloud Manager documentation.

Preparing your networking

The Service Connector needs a connection to your ONTAP clusters, to AWS S3, and to the Cloud Tiering service.

Steps

1. Set up an on-premises location 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 S3
   - An HTTPS connection over port 443 to your ONTAP clusters
2. Ensure that outbound internet access is allowed to those endpoints:
   - http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
   - https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
   - https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

     The installer accesses these URLs during the installation process.

Providing permissions to an AWS account

After you install the Service Connector, you need to provide access keys for an AWS account. That account needs specific permissions so the Service Connector can set up data tiering to AWS S3 on your behalf.

Cloud Tiering tiers data to an S3 bucket that resides in this AWS account.

Steps

1. From the AWS IAM console, create an IAM policy by copying and pasting the permissions below.

   For step-by-step instructions, refer to AWS Documentation: Creating IAM Policies.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:DecodeAuthorizationMessage",
                "s3:ListBucket",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:CreateBucket",
                "s3:GetBucketTagging",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::fabric-pool*"
        }
    ]
}
```

2. Attach the policy to an IAM role or an IAM user.

   For step-by-step instructions, refer to the following:

   - AWS Documentation: Creating IAM Roles
   - AWS Documentation: Adding and Removing IAM Policies

Result

The account now has the required permissions. You need to provide access keys for the AWS account after you install the Service Connector.

Installing the Service Connector on an on-premises Linux host

After you verify system and network requirements, download and install the software on a supported Linux host.

About this task

- Root privileges are not required for installation.
- The Service Connector installs the AWS command line tools (awscli) to enable recovery procedures from NetApp support.

  If you receive a message that installing the awscli failed, you can safely ignore the message. The Service Connector can operate successfully without the tools.

- The installer that is available on the NetApp Support Site might be an earlier version. After installation, the software automatically updates itself if a new version is available.

Steps

1. Download the installation script for Cloud Manager 3.8.4 or later from the NetApp Support Site, and then copy it to the Linux host.

   Why do I need to install Cloud Manager?

2. Assign permissions to execute the script.

   Example

   ```
   chmod +x OnCommandCloudManager-V3.8.4.sh
   ```

3. Run the installation script:

   ```
   ./OnCommandCloudManager-V3.8.4.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent runs the installation without prompting you for information.

   proxy is required if the host is behind a proxy server.

   proxyport is the port for the proxy server.

   proxyuser is the user name for the proxy server, if basic authentication is required.

   proxypwd is the password for the user name that you specified.

4. Unless you specified the silent parameter, type **Y** to continue the script, and then enter the HTTP and HTTPS ports when prompted.

   If you change the HTTP and HTTPS ports, you must ensure that users can access the Cloud Manager web console from a remote host:

   - Modify the security group to allow inbound connections through the ports.
   - Specify the port when you enter the URL to the web console.

The Service Connector is now installed. At the end of the installation, the Cloud Manager service (occm) restarts twice if you specified a proxy server.

5. Open a web browser and enter the following URL:

   https://*ipaddress*:*port*

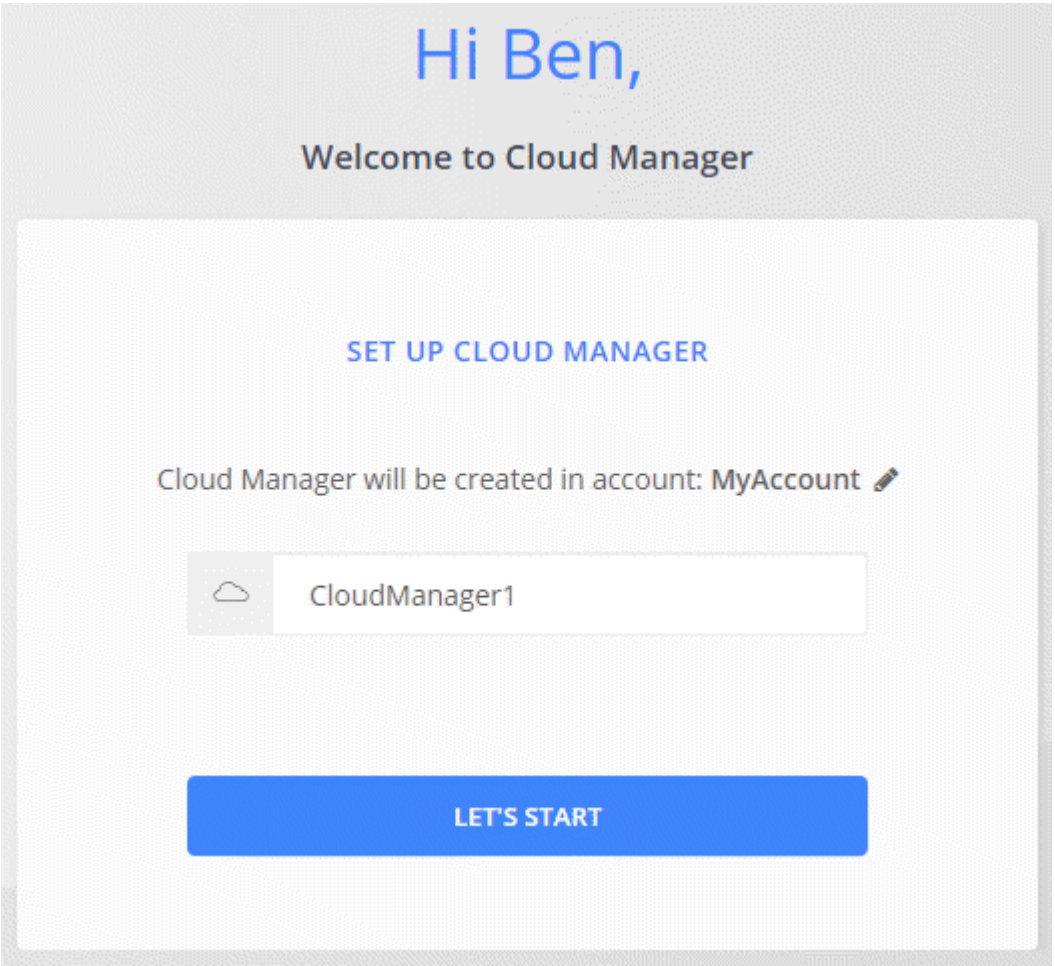
   ipaddress can be localhost, a private IP address, or a public IP address, depending on the configuration of the host.

   port is required if you changed the default HTTP (80) or HTTPS (443) ports. For example, if the HTTPS port was changed to 8443, you would enter https://*ipaddress*:8443

6. Sign up at NetApp Cloud Central or log in.
7. After you log in, set up Cloud Manager:
   a. Specify the Cloud Central account to associate with this Cloud Manager system. This should be the same account that you specified when you ran the pre-installation script.

      Learn about Cloud Central accounts.

   b. Enter a name for the system.



After you finish

Add an AWS account to Cloud Manager that has the required permissions.

Adding the AWS account to Cloud Manager

After you provide an AWS account with the required permissions, you need to add AWS access keys to Cloud Manager. This enables the Service Connector to set up data tiering to AWS S3 on your behalf.

Cloud Tiering tiers data to an S3 bucket that resides in this AWS account.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Click **Add Credentials** and select **AWS**.
3. Select **AWS keys**.
4. Confirm that the policy requirements have been met and then click **Create Account**.

Result

The Service Connector is now installed with the permissions that it needs to tier cold data from your ONTAP systems to AWS S3. You should now see the Service Connector when you set up tiering to a new cluster.

Tiering inactive data from your first cluster to AWS S3

After you prepare your AWS 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.

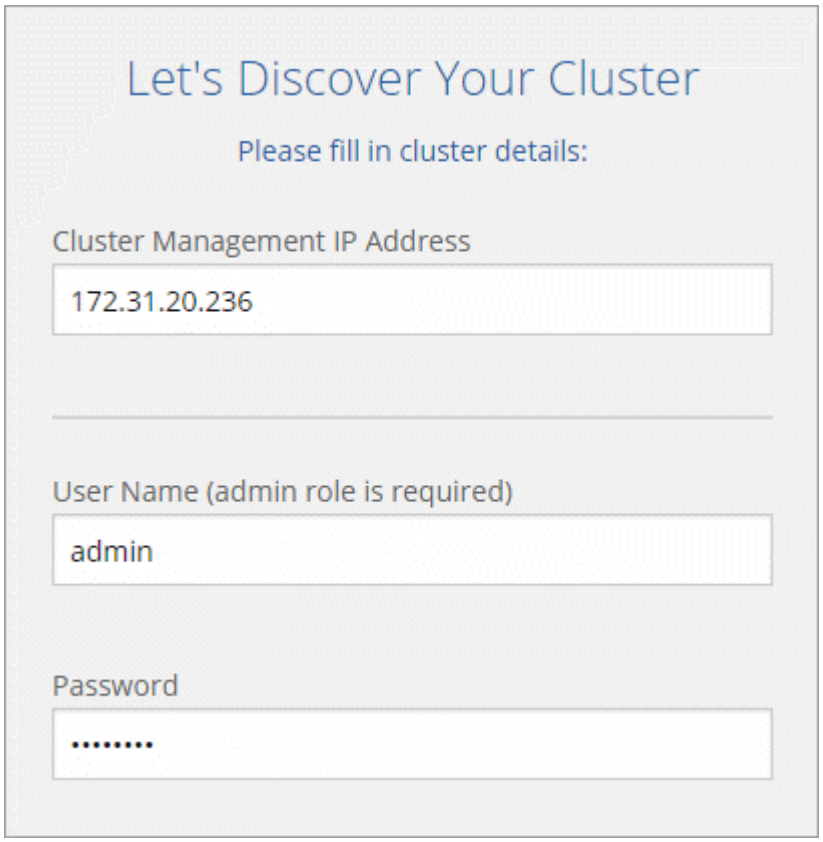
    The Service Connector uses this account to send API operations to the ONTAP cluster.
- To deploy the Service Connector in AWS, you'll need the following:
  - The AWS region, VPC, and subnet in which the Service Connector will reside.
  - An AWS access key for an IAM user who has the required permissions.
- To set up tiering to S3, you'll need an AWS access key for an IAM user who has the required S3 permissions.

If you haven't met these requirements, see Preparing your environment.

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 AWS:

   - **Select Provider**: Select **Amazon Web Services** as the target location for the Service Connector.
   - **AWS Credentials**: Enter the AWS access key ID and secret key for an IAM user that has the required permissions to deploy the Service Connector.
   - **Location**: Select the AWS region, VPC, and subnet for the Service Connector EC2 instance.

     Remember, the Service Connector must have a constant connection to the ONTAP cluster and a constant internet connection to the Cloud Tiering service.

- **Network**: Select a key pair to use for the EC2 instance, choose whether to assign a public IP, and specify an HTTP proxy, if one is required for outbound connectivity.
- **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. **S3 Bucket**: Add a new S3 bucket or select an existing S3 bucket that starts with the prefix *fabric-pool* and click **Continue**.

      The *fabric-pool* prefix is required because the IAM policy for the Service Connector enables the instance to perform S3 actions on buckets named with that exact prefix.

      For example, you could name the S3 bucket fabric-pool-AFF1, where AFF1 is the name of the cluster.

   b. **Storage Class**: Select the S3 storage class that you want to transition the data to after 30 days and click **Continue**.

      If you choose Standard, then the data remains in that storage class.

   c. **Credentials**: Enter the access key ID and secret key for an IAM user who has the required S3 permissions.

      The IAM user must be in the same AWS account as the bucket that you selected or created on the **S3 Bucket** page.

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

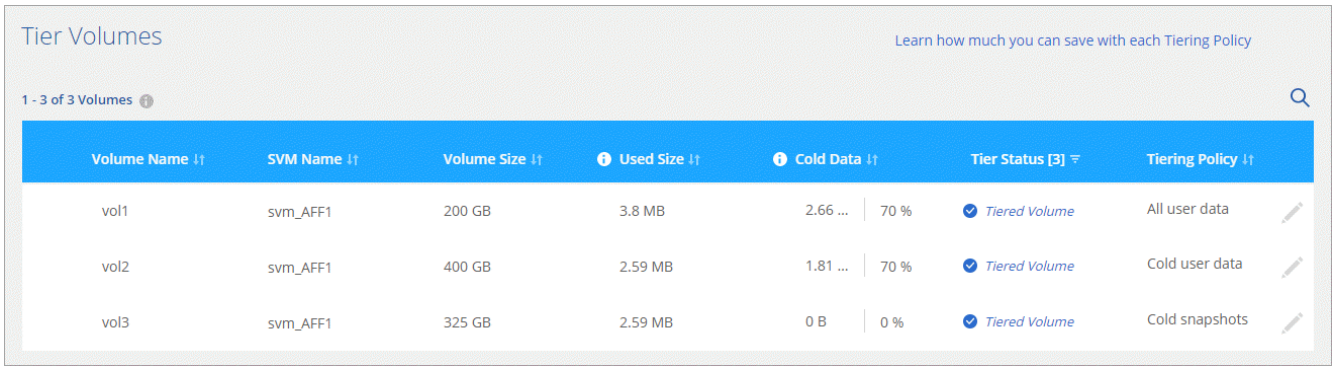
      Selecting the correct IPspace ensures that Cloud Tiering can set up a connection from ONTAP to your cloud provider's object storage.

      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 S3 object storage.

What's next?

Be sure to subscribe to the Cloud Tiering service from the AWS 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 S3 storage classes and regions

Cloud Tiering supports several S3 storage classes and most regions.

Supported S3 storage classes

Cloud Tiering can apply a lifecycle rule so the data transitions from the *Standard* storage class to another storage class after 30 days. You can choose from the following storage classes:

- Standard-Infrequent Access
- One Zone-IA
- Intelligent

If you choose Standard, then the data remains in that storage class.

Learn about S3 storage classes.

Supported AWS regions

Cloud Tiering supports the following AWS regions.

Asia Pacific

- Mumbai
- Seoul
- Singapore
- Sydney
- Tokyo

Europe

- Frankfurt
- Ireland
- London
- Paris
- Stockholm

North America

- Canada Central
- GovCloud (US-West) – starting with ONTAP 9.3
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)

South America

- São Paulo