



Use Cloud Tiering

Cloud Tiering

NetApp
June 24, 2022

Table of Contents

- Use Cloud Tiering 1
 - Measure network latency and throughput performance 1
 - Managing data tiering from your clusters 2
 - Get an overview of data tiering from your clusters 9
 - Reference 10

Use Cloud Tiering

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

Node: aff-01 ▼ Last check: 01/13/2021 04:25 pm ↻ Recheck performance

Operation	Size	Avg. Latency (ms)	Throughput
PUT	4 MB	502	408.06 MB
GET	4 KB	79	15.05 MB
GET	8 KB	197	28.35 MB
GET	32 KB	291	109.71 MB
GET	256 KB	361	714.39 MB

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. At the top of Cloud Manager, click **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. At the top of Cloud Manager, click **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.

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

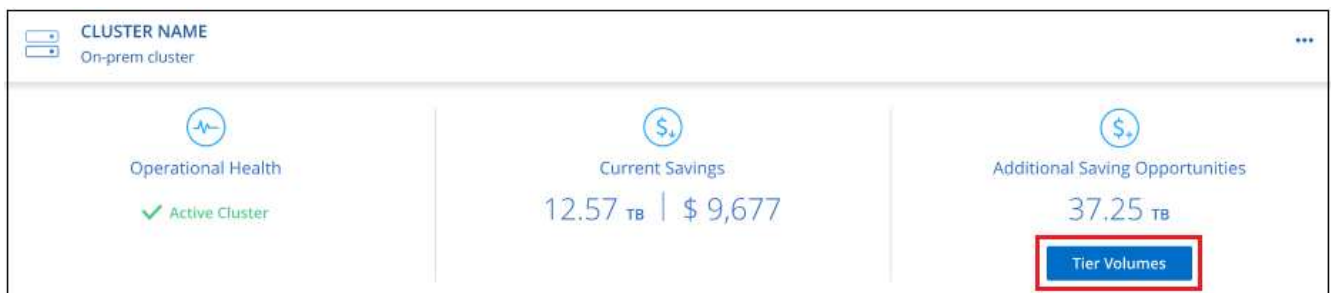
Set up data tiering for additional volumes at any time—for example, after creating a new volume.




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.

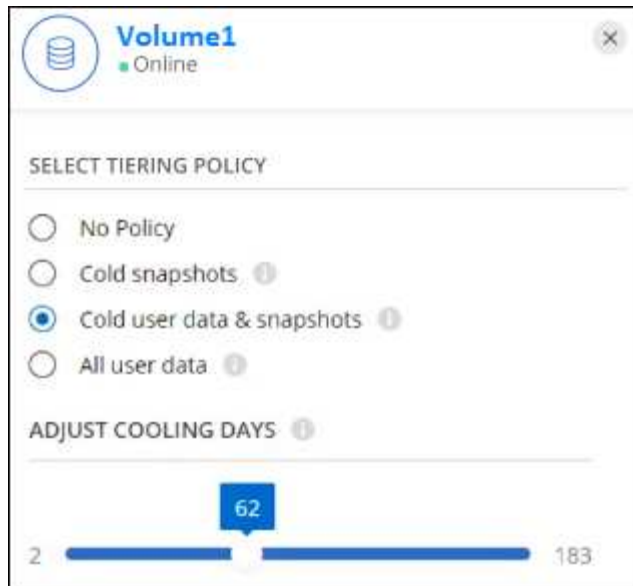
Steps

1. At the top of Cloud Manager, click **Tiering**.
2. From the **Cluster Dashboard**, click **Tier Volumes** 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.](#)



Result

The selected volumes start to have their data tiered to the cloud.

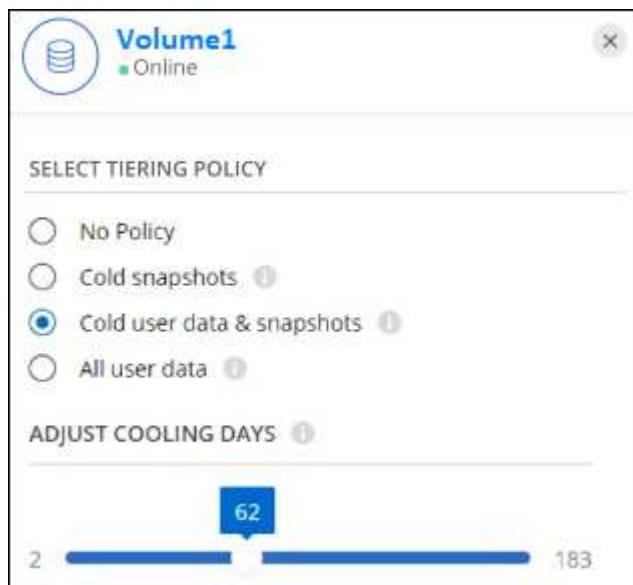
Changing a volume's tiering policy

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. At the top of Cloud Manager, click **Tiering**.
2. From the **Cluster 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:


Option	Description	Affect on Tiering Policy
Bring back all data	Retrieves all volume data and Snapshot copies tiered in the cloud and promotes them to the performance tier.	Tiering policy is changed to "No policy".
Bring back active file system	Retrieves only active file system data tiered in the cloud and promotes it to the performance tier (Snapshot copies remain in the cloud).	Tiering policy is changed to "Cold snapshots".

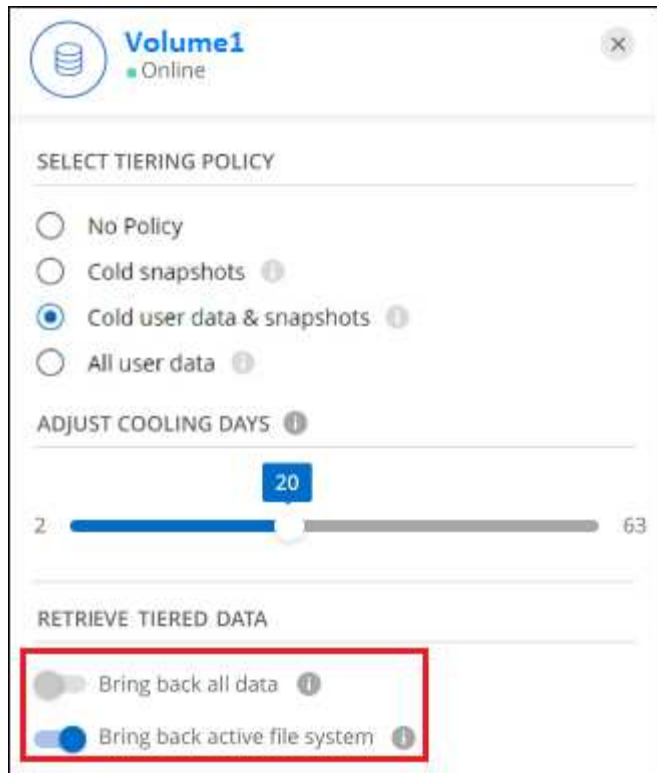


You may be charged by your cloud provider based on that amount of data transferred off the cloud.

Steps

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

1. At the top of Cloud Manager, click **Tiering**.
2. From the **Cluster Dashboard**, click **Tier Volumes** for the cluster.
3. Click the  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.

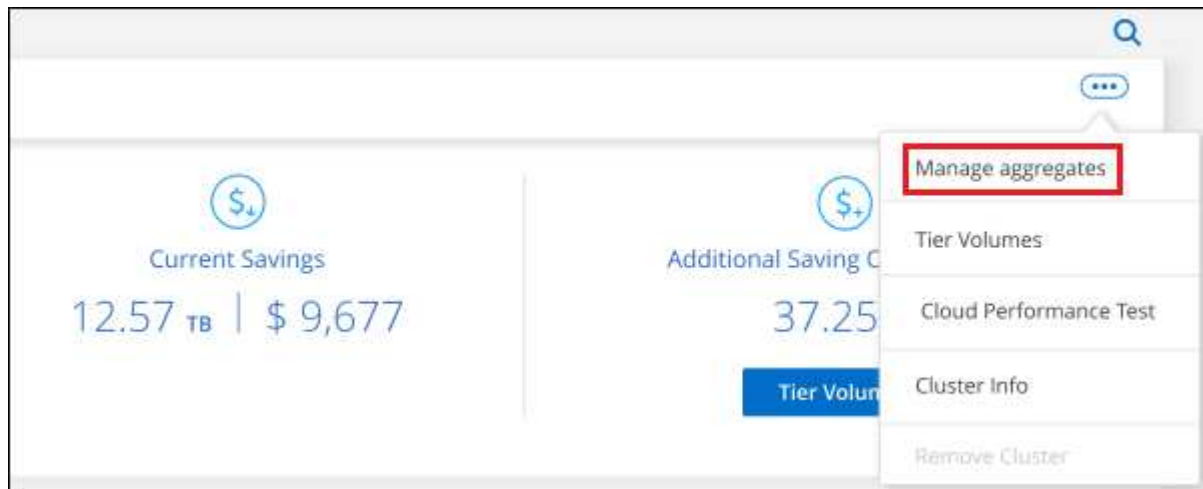



It's best to keep IDR enabled because it helps to identify your inactive data and savings opportunities. IDR must remain enabled if data tiering was enabled on an aggregate.

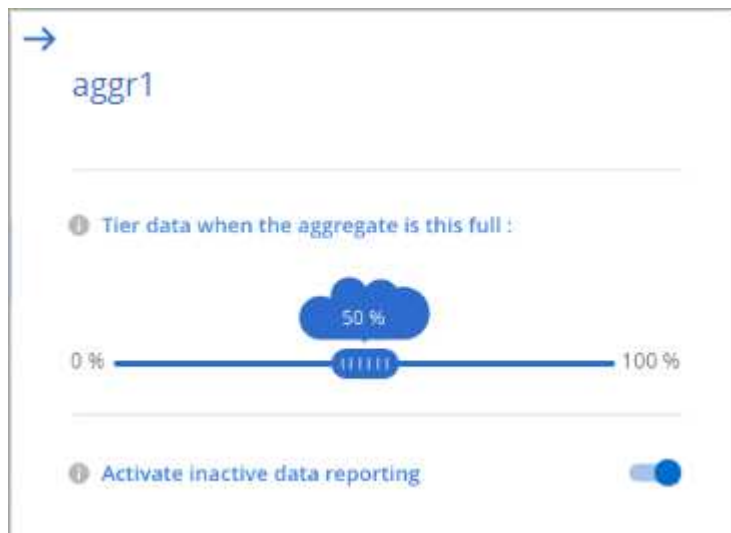
Steps

1. At the top of Cloud Manager, click **Tiering**.

2. From the **Cloud Tiering** page, click the menu icon for a cluster and select **Manage Aggregates**.



3. On the **Manage Aggregates** page, click the  icon for an aggregate in the table.
4. Modify the fullness threshold and choose whether to enable or disable inactive data reporting.



5. Click **Apply**.

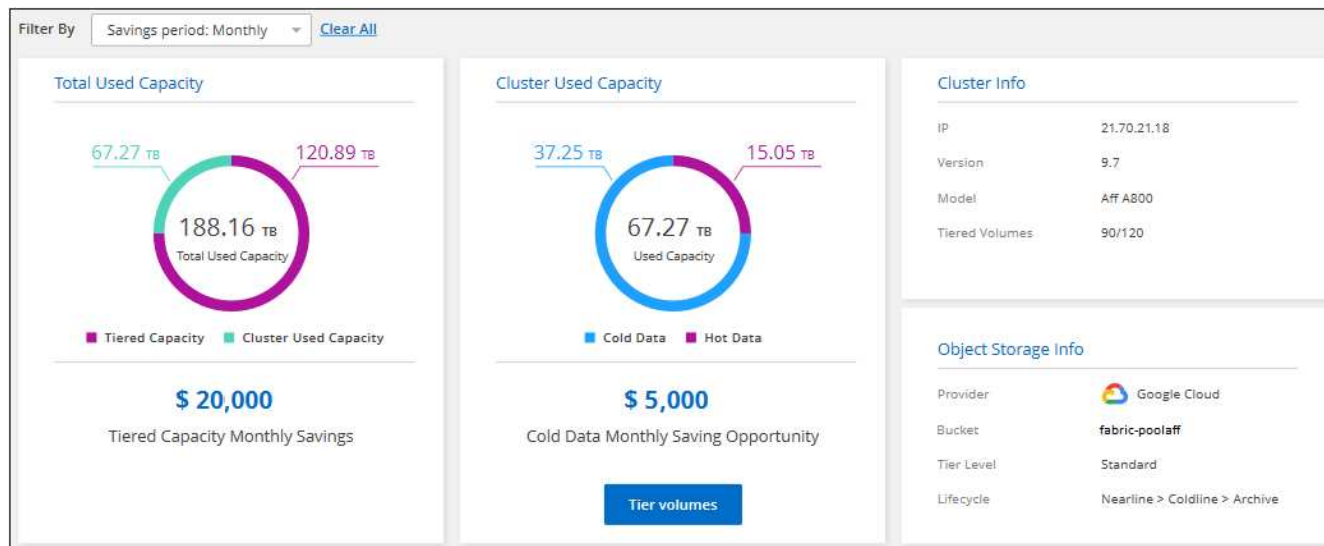
Reviewing tiering info for a cluster

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.

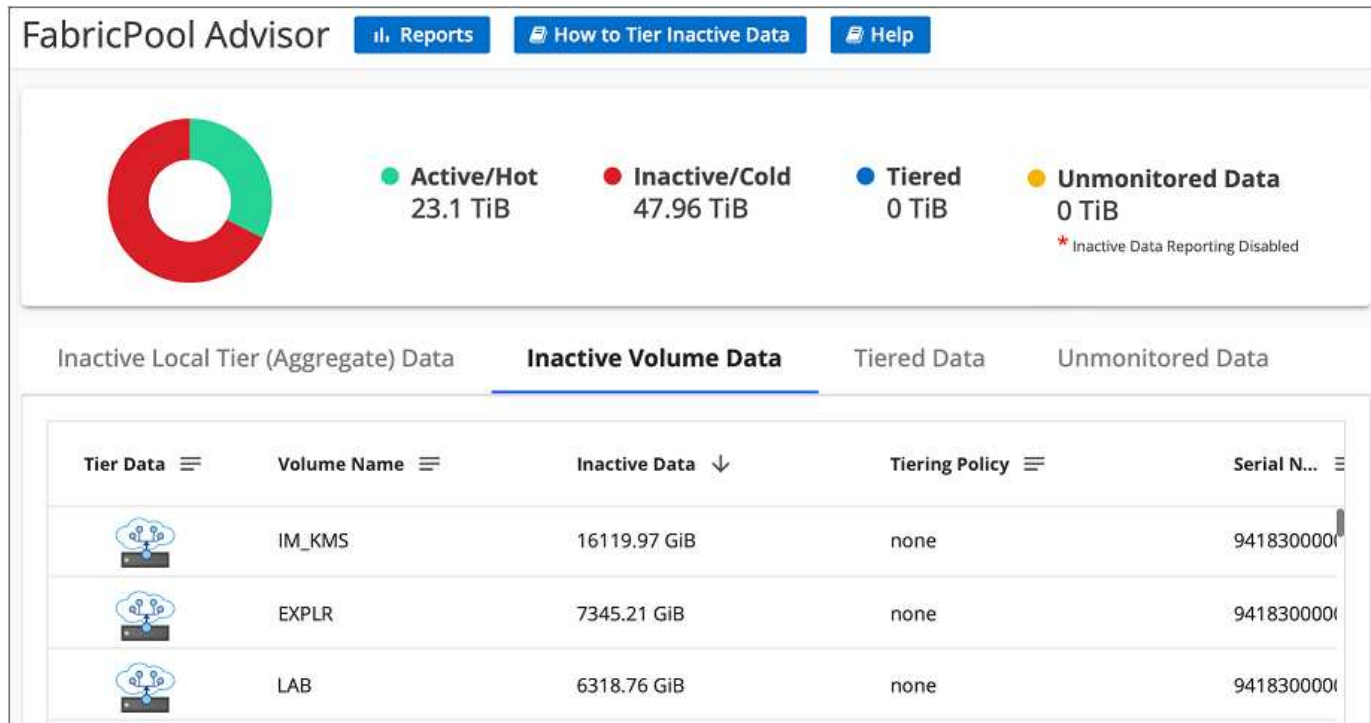
Steps

1. At the top of Cloud Manager, click **Tiering**.
2. From the **Cluster Dashboard**, click the menu icon for a cluster and select **Cluster info**.
3. Review details about the cluster.

Here's an example:



You can also [view tiering information for a cluster from Active IQ Digital Advisor](#) if you're familiar with this NetApp product. Just select **FabricPool Advisor** from the left navigation pane.

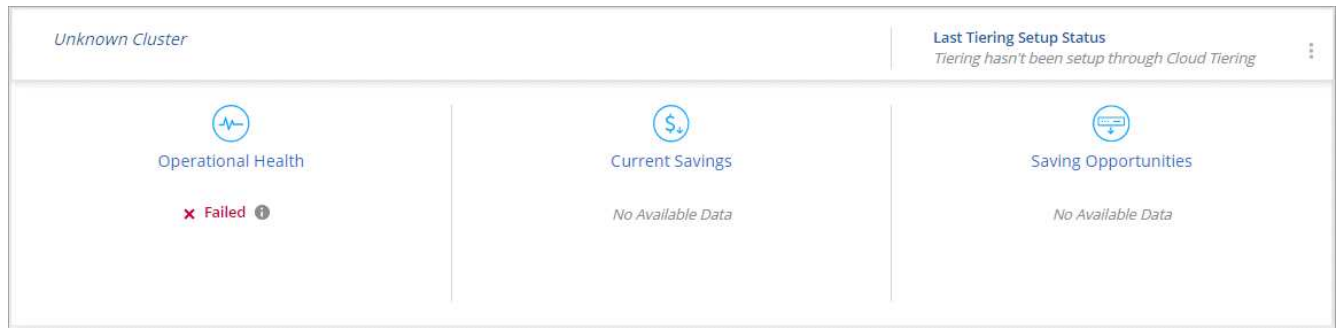


Fixing operational health

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 Cloud Manager.

Steps

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



2. Hover over the **i** 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 Cloud Manager 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 Cloud Manager 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

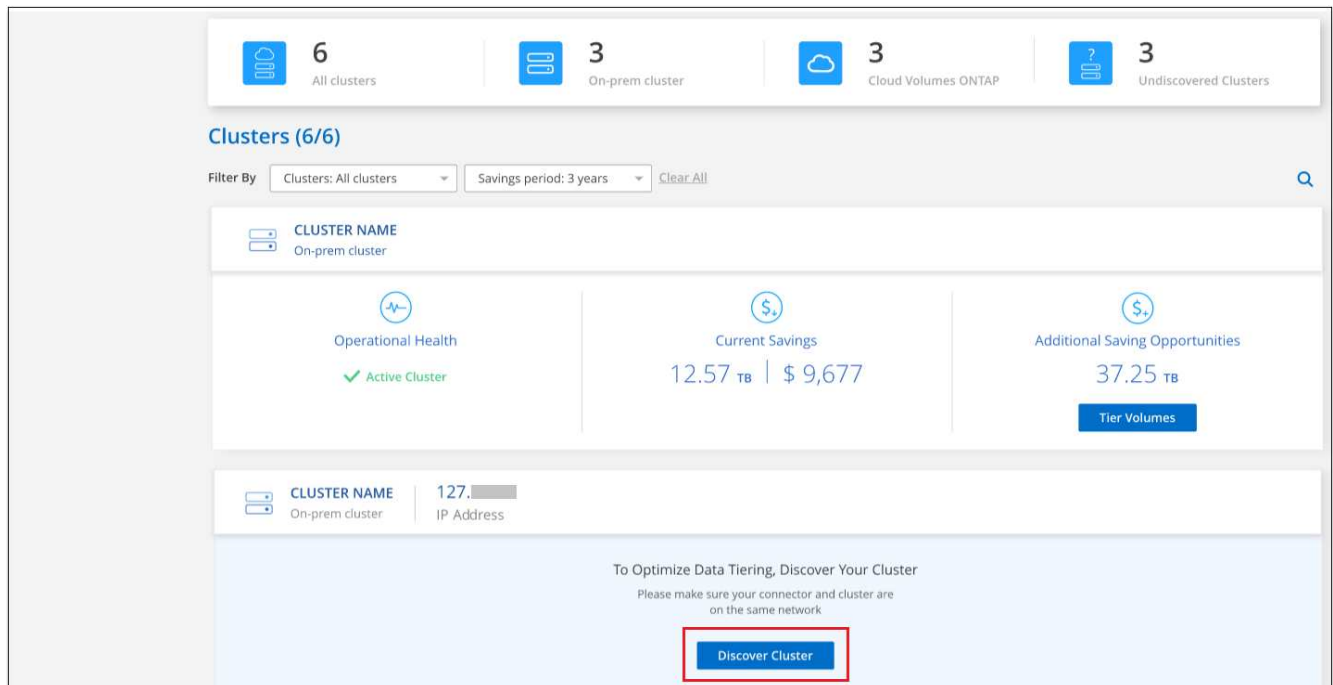
1. From Cloud Tiering, click the **Cluster Dashboard** tab.
2. To see any undiscovered clusters, click **Show Undiscovered Clusters**.



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

If your NSS credentials are not saved in Cloud Manager, 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 Cloud Manager 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

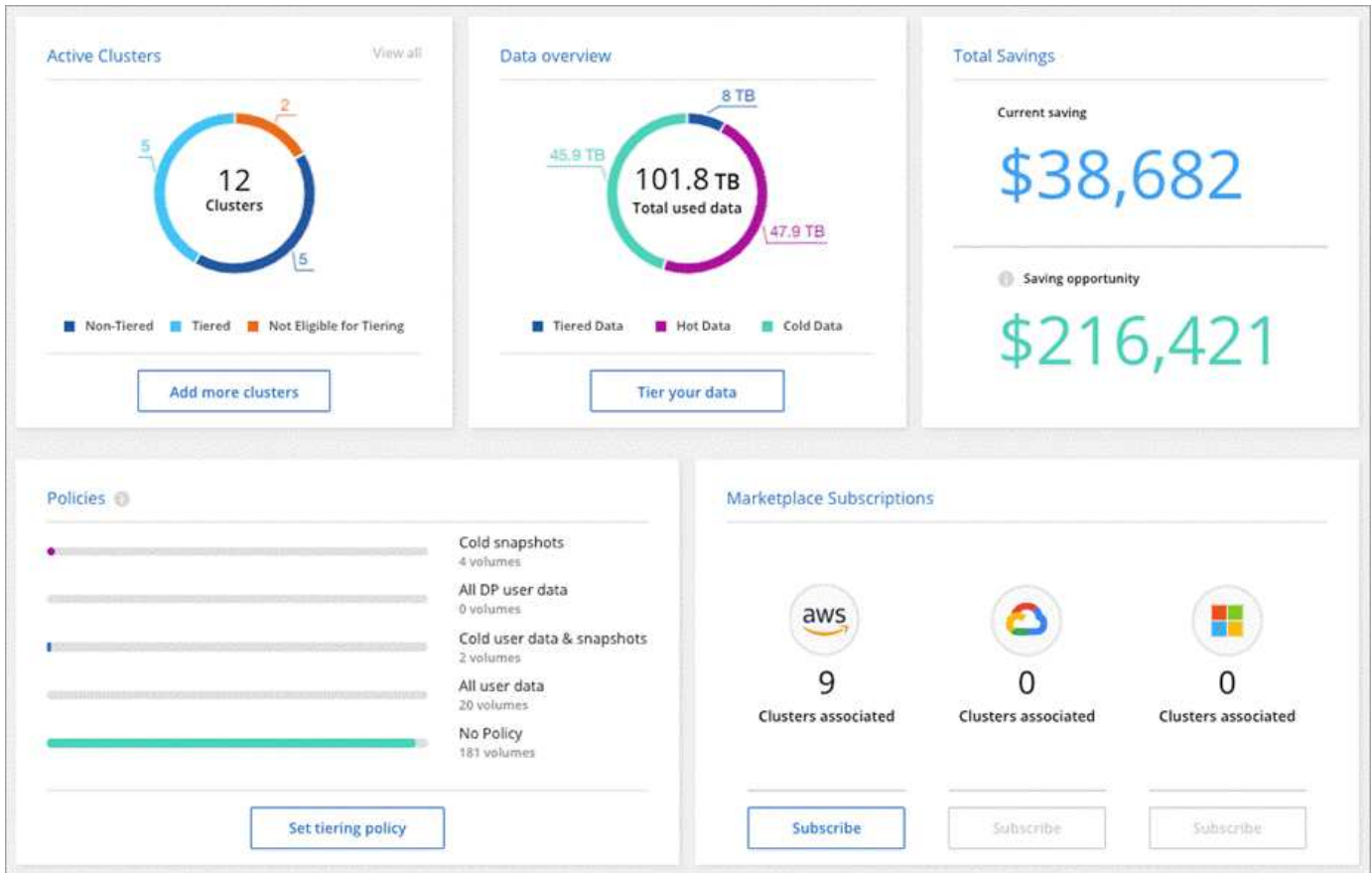
Cloud Manager discovers the cluster and adds it to a working environment in the Canvas using the cluster name as the working environment name.

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

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.

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.

Steps

1. Click **Tiering > On-Prem Overview**.

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

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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.