Tiering data from on-premises ONTAP clusters to Amazon S3

Cloud Manager

Ben Cammett
May 18, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_tiering_onprem_aws.html on June 15, 2020.
Always check docs.netapp.com for the latest.

NetApp®

Table of Contents

Tiering data from on-premises ONTAP clusters to Amazon S3 1
Quick start 1
Requirements 1
Tiering inactive data from your first cluster to Amazon S3 4

Tiering data from on-premises ONTAP clusters to Amazon S3

Free space on your on-prem ONTAP clusters by tiering data to Amazon S3. Data tiering is powered by NetApp's Cloud Tiering service.

Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

Prepare to tier data to Amazon S3

You need the following:

- An AFF or FAS system with all-SSD aggregates that's running ONTAP 9.2 or later and has an HTTPS connection to Amazon 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 S3.
- Cloud Manager installed in an AWS VPC or on your premises.
- Networking for Cloud Manager that enables an outbound HTTPS connection to the ONTAP cluster, to S3 storage, and to the Cloud Tiering service.

Set up tiering

Select an on-prem working environment, click **Setup Tiering** and follow the prompts to tier data to Amazon S3.

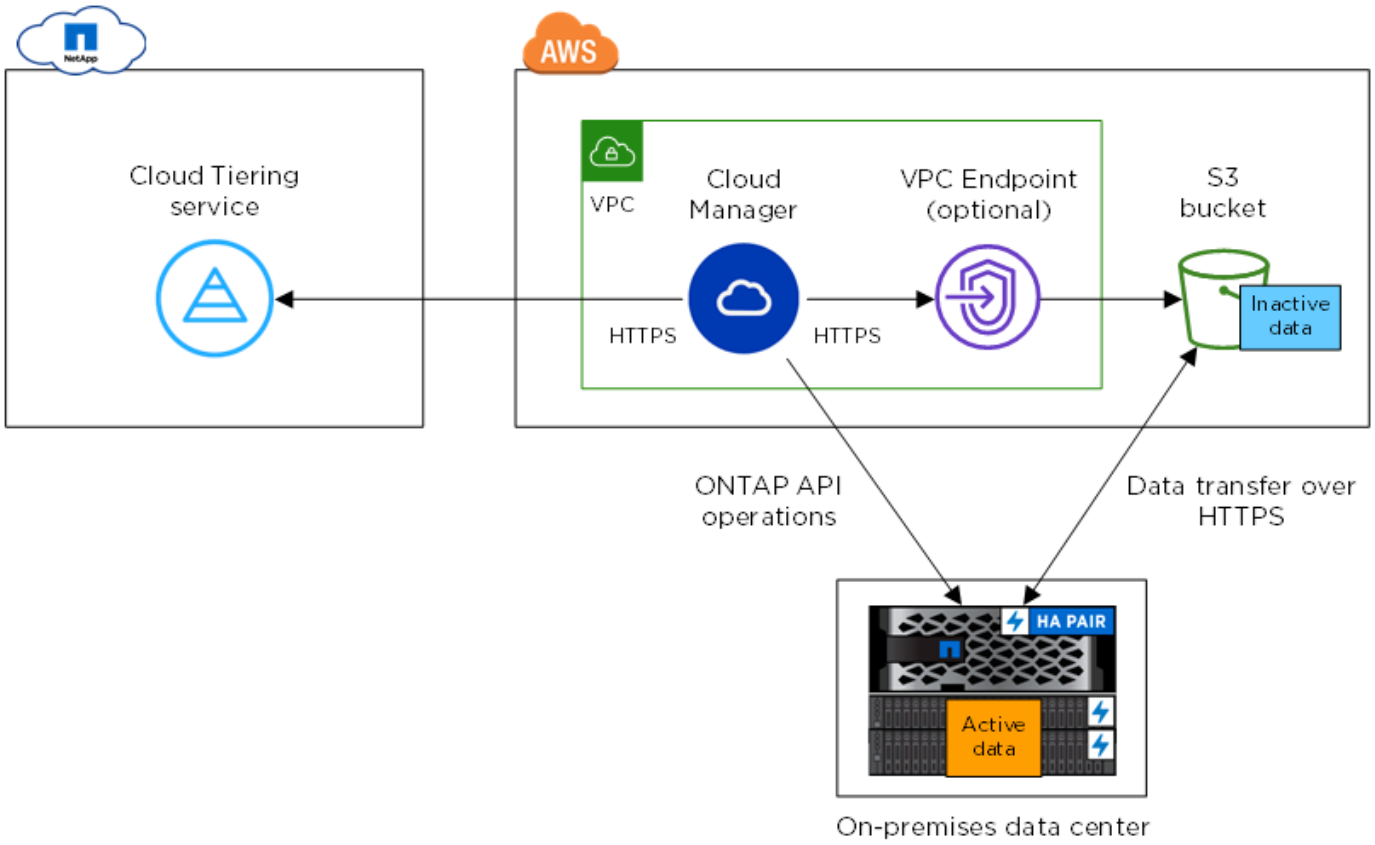
Set up licensing

Pay for Cloud Tiering through a pay-as-you-go subscription, an ONTAP tiering license, or a combination of both. Licensing isn't available from within Cloud Manager, but you can go directly to the Cloud Tiering service to set it up.

Requirements

Verify support for your ONTAP cluster, set up your networking, and prepare your object storage.

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



Communication between Cloud Manager and S3 is for object storage setup only. Cloud Manager 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 Amazon 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 Amazon 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's not required between the ONTAP cluster and S3. Because performance is significantly better when using AWS Direct Connect, doing so is the recommended best practice.

- An inbound connection is required from Cloud Manager, 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.

Preparing networking for Cloud Manager

Ensure that Cloud Manager has the required networking connections. Cloud Manager can be installed on-prem or in AWS.

Steps

1. Ensure that the network where Cloud Manager is installed 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. 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 Cloud Manager and S3 to stay in your AWS internal network.

Preparing Amazon S3

When you set up data tiering to a new cluster, you're prompted to create an S3 bucket or to select an existing S3 bucket in the AWS account where Cloud Manager is set up.

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

Tiering inactive data from your first cluster to Amazon S3

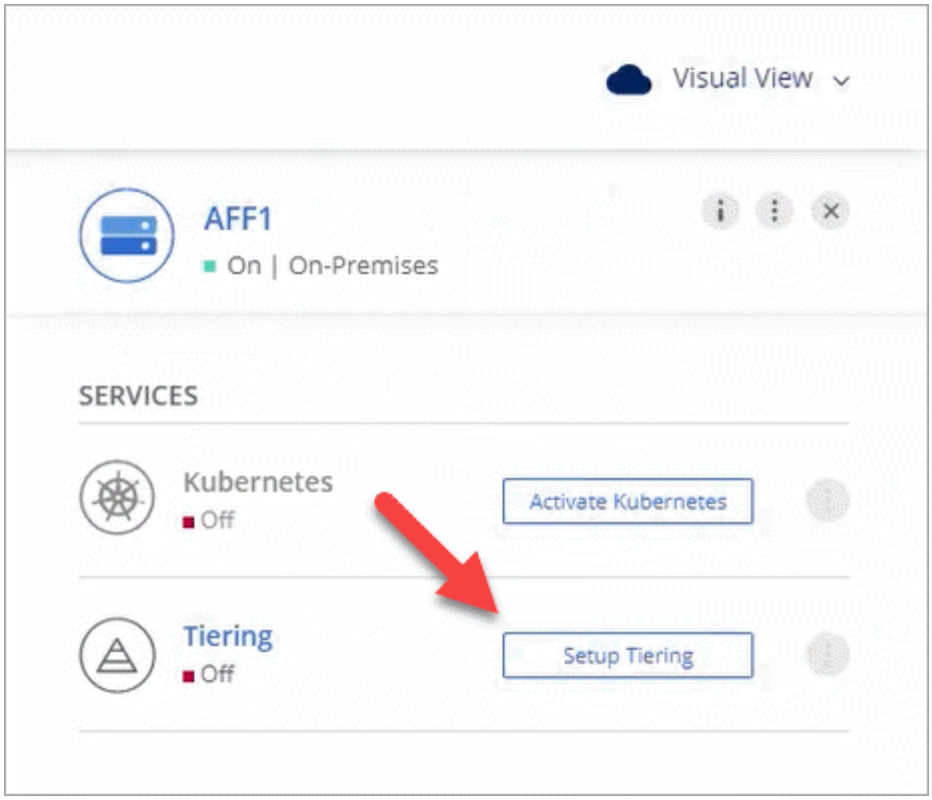
After you prepare your AWS environment, start tiering inactive data from your first cluster.

What you'll need

- An on-premises working environment.
- An AWS access key for an IAM user who has the required S3 permissions.

Steps

1. Select an on-prem cluster.
2. Click **Setup Tiering**.



You're now on the Tiering dashboard.

3. Click **Set up Tiering** next to the cluster.
4. 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.

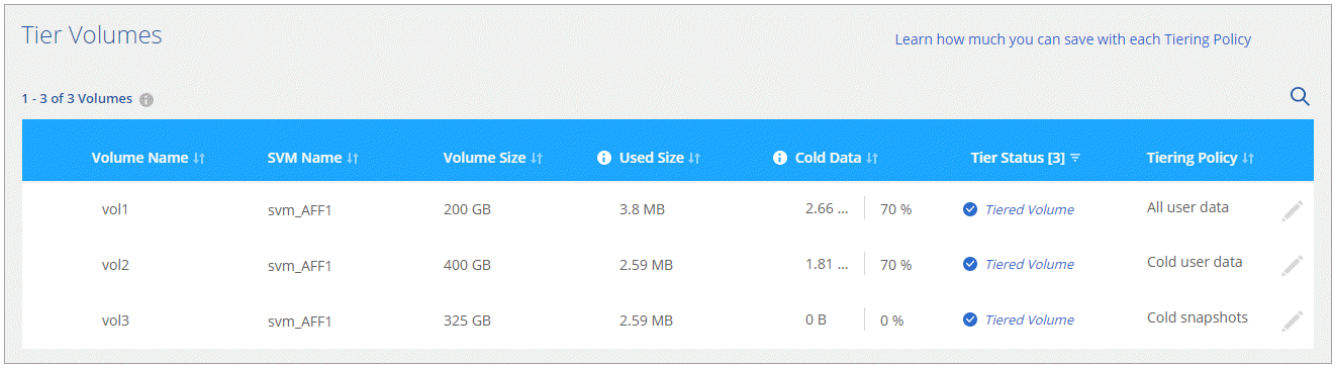
      The IAM user must be in the same AWS account as the bucket that you selected or created on the **S3 Bucket** page.

   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.

5. Click **Continue** to select the volumes that you want to tier.
6. On the **Tier Volumes** page, set up tiering for each volume. Click the icon, select a tiering policy, optionally adjust the cooling days, and click **Apply**.

   Learn more about volume tiering policies.



Result

You've successfully set up data tiering from volumes on the cluster to S3 object storage.

What's next?

Be sure to subscribe from the Cloud Tiering service.

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.

Copyright Information

Copyright © 2020 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.