Tiering inactive data to low-cost object storage

Cloud Manager

Ben Cammett
May 29, 2020

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

Table of Contents

Tiering inactive data to low-cost object storage 1
Configurations that support data tiering 1
Requirements to tier cold data to AWS S3 2
Requirements to tier cold data to Azure Blob storage 2
Requirements to tier cold data to a Google Cloud Storage bucket 3
Tiering data from read-write volumes 3
Tiering data from data protection volumes 4
Changing the storage class for tiered data 4

Tiering inactive data to low-cost object storage

You can reduce storage costs by combining an SSD or HDD performance tier for hot data with an object storage capacity tier for inactive data. For a high-level overview, see Data tiering overview.

To set up data tiering, you simply need to do the following:

Choose a supported configuration

Most configurations are supported. If you have a Cloud Volumes ONTAP Standard, Premium, or BYOL system running the most recent version, then you should be good to go. Learn more.

Ensure connectivity between Cloud Volumes ONTAP and object storage

- For AWS, you'll need a VPC Endpoint to S3. Learn more.
- For Azure, you won't need to do anything as long as Cloud Manager has the required permissions. Learn more.
- For GCP, you need to configure the subnet for Private Google Access and set up a service account. Learn more.

Choose a tiering policy when creating, modifying, or replicating a volume

Cloud Manager prompts you to choose a tiering policy when you create, modify, or replicate a volume.

- Tiering data on read-write volumes
- Tiering data on data protection volumes

What's not required for data tiering

- You don't need to install a feature license to enable data tiering.
- You don't need to create the capacity tier (an S3 bucket, Azure Blob container, or GCP bucket). Cloud Manager does that for you.

Configurations that support data tiering

You can enable data tiering when using specific configurations and features:

- Data tiering is supported with Cloud Volumes ONTAP Standard, Premium, and BYOL, starting with

the following versions:

- Version 9.2 in AWS
- Version 9.4 in Azure with single node systems
- Version 9.6 in Azure with HA pairs
- Version 9.6 in GCP

Data tiering is not supported in Azure with the DS3_v2 virtual machine type.

- In AWS, the performance tier can be General Purpose SSDs, Provisioned IOPS SSDs, or Throughput Optimized HDDs.
- In Azure, the performance tier can be Premium SSD managed disks, Standard SSD managed disks, or Standard HDD managed disks.
- In GCP, the performance tier can be either SSDs or HDDs (standard disks).
- Data tiering is supported with encryption technologies.
- Thin provisioning must be enabled on volumes.

Requirements to tier cold data to AWS S3

Ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, see AWS Documentation: Creating a Gateway Endpoint.

When you create the VPC Endpoint, be sure to select the region, VPC, and route table that corresponds to the Cloud Volumes ONTAP instance. You must also modify the security group to add an outbound HTTPS rule that enables traffic to the S3 endpoint. Otherwise, Cloud Volumes ONTAP cannot connect to the S3 service.

If you experience any issues, see AWS Support Knowledge Center: Why can't I connect to an S3 bucket using a gateway VPC endpoint?.

Requirements to tier cold data to Azure Blob storage

You don't need to set up a connection between the performance tier and the capacity tier as long as Cloud Manager has the required permissions. Cloud Manager enables a VNet service endpoint for you if the Cloud Manager policy has these permissions:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

The permissions are included in the latest Cloud Manager policy.

Requirements to tier cold data to a Google Cloud Storage bucket

- The subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access. For instructions, refer to Google Cloud Documentation: Configuring Private Google Access.
- Cloud Volumes ONTAP 9.7: You need to create a service account that has the predefined Storage Admin role. You'll need to select this service account when you create a Cloud Volumes ONTAP working environment. For more details, see step 3 in Getting started with Cloud Volumes ONTAP in Google Cloud Platform.

  If you don't enable data tiering and select a service account when you create the Cloud Volumes ONTAP 9.7 system, then you'll need to turn off the system and add the service account to Cloud Volumes ONTAP from the GCP console.

- Cloud Volumes ONTAP 9.6: You need to add a Google Cloud Platform account to Cloud Manager by entering storage access keys for a service account. The keys enable Cloud Manager to set up a Cloud Storage bucket for data tiering. For instructions, see Setting up and adding GCP accounts for data tiering with 9.6.

Tiering data from read-write volumes

Cloud Volumes ONTAP can tier inactive data on read-write volumes to cost-effective object storage, freeing up the performance tier for hot data.

Steps

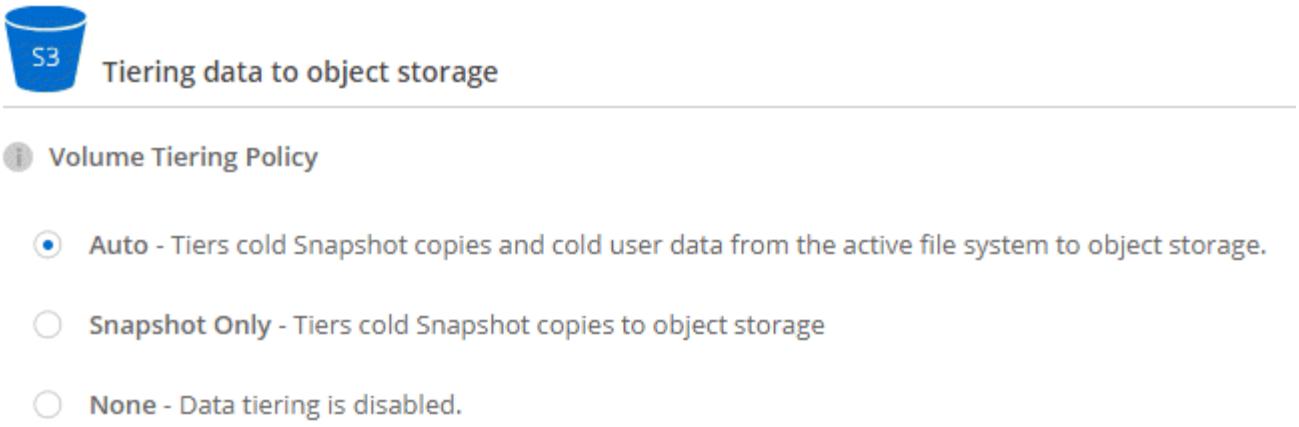
1. In the working environment, create a new volume or change the tier of an existing volume:

Task	Action
Create a new volume	Click **Add New Volume**.
Modify an existing volume	Select the volume and click **Change Disk Type & Tiering Policy**.

2. Select the Snapshot Only policy or the Auto policy.

   For a description of these policies, see Data tiering overview.

   Example



Cloud Manager creates a new aggregate for the volume if a data tiering-enabled aggregate does not already exist.

If you prefer to create aggregates yourself, you can enable data tiering on aggregates when you create them.

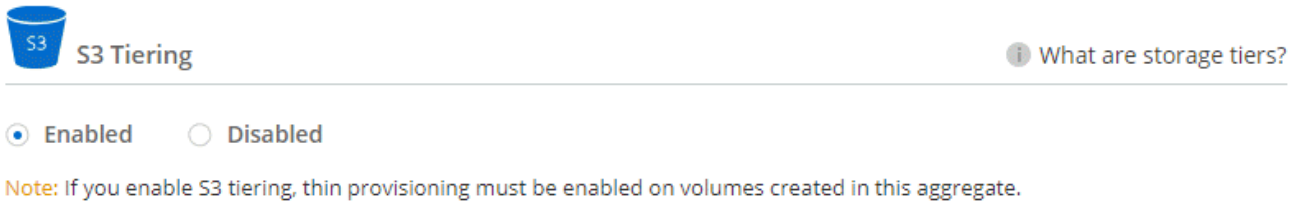
Tiering data from data protection volumes

Cloud Volumes ONTAP can tier data from a data protection volume to a capacity tier. If you activate the destination volume, the data gradually moves to the performance tier as it is read.

Steps

1. On the Working Environments page, select the working environment that contains the source volume, and then drag it to the working environment to which you want to replicate the volume.
2. Follow the prompts until you reach the tiering page and enable data tiering to object storage.

Example



For help with replicating data, see Replicating data to and from the cloud.

Changing the storage class for tiered data

After you deploy Cloud Volumes ONTAP, you can reduce your storage costs by changing the storage class for inactive data that hasn't been accessed for 30 days. The access costs are higher if you do

access the data, so you must take that into consideration before you change the storage class.

The storage class for tiered data is system wide—it's not per volume.

For information about supported storage classes, see Data tiering overview.

Steps

1. From the working environment, click the menu icon and then click **Storage Classes** or **Blob Storage Tiering**.
2. Choose a storage class and then click **Save**.

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.