



Extend to the cloud

ONTAP 9

NetApp
July 15, 2021

This PDF was generated from https://docs.netapp.com/us-en/ontap/task_add_connection_to_cloud.html on July 15, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Extend to the cloud. 1
 - Cloud overview. 1
 - Add a connection to the cloud 2
 - Tier data to cloud 2
 - Tier data to local bucket 3
 - Create tags for tiering objects 4
 - Enable inactive data reporting 4
 - Back up data using the Cloud Backup Service 4
 - Manage the connection to the Cloud Backup Service 7

Extend to the cloud

The topics in this section show you how to configure and manage a cloud tier with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to configure and manage a cloud tier, see this content:

- [Managing Storage Tiers By Using FabricPool](#)
- [S3 Configuration Power Guide](#)

If you are using legacy OnCommand System Manager for ONTAP 9.5-9.7 releases to configure and manage a cloud tier, see the content for your ONTAP release:

- [Cluster management using System Manager 9.6 and 9.7](#)
- [Cluster management using System Manager 9.5](#)

Cloud overview

You can use FabricPool to automatically tier data depending on how frequently the data is accessed.

FabricPool is a hybrid storage solution that uses an all flash (all SSD) aggregate as the performance tier and an object store as the cloud tier. Using a FabricPool helps you reduce storage cost without compromising performance, efficiency, or protection.

The cloud tier can be located on NetApp StorageGRID or ONTAP S3 (beginning with ONTAP 9.8), or one of the following service providers:

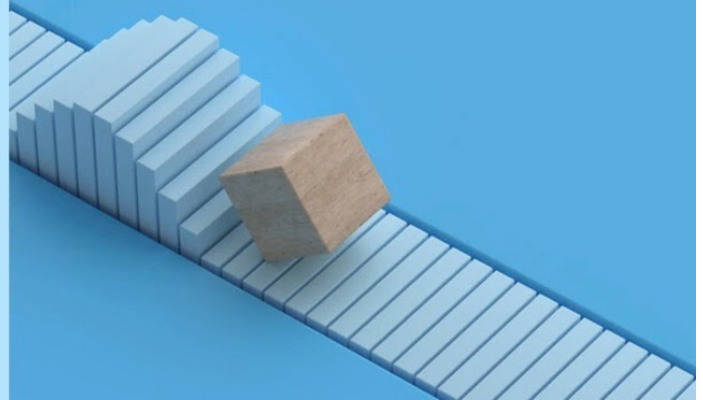
- Alibaba cloud
- Amazon S3
- Google Cloud
- IBM cloud
- Microsoft Azure Blob Storage

ONTAP FabricPool

Tier Data and Lower Costs

Use Case

© 2020 NetApp, Inc. All rights reserved.



Add a connection to the cloud

Starting with ONTAP 9.9.0, you can use System Manager to add a connection to the cloud.

You start by using NetApp Cloud Insights to configure a collector. During the configuration process, you copy a pairing code that is generated by Cloud Insights, and then you log on to a cluster using System Manager. There, you add a cloud connection using that pairing code. The rest of the process is completed in Cloud Insights.

Steps

1. In Cloud Insights, during the process to configure a collector, copy the generated pairing code.
2. Using System Manager 9.9.0 or later, log on to the cluster.
3. Go to **Cluster > Settings**.
4. In the Cloud Connections section, select **Add** to add a connection.
5. Enter a name for the connection, and paste the pairing code in the space provided.
6. Click **Add**.
7. Return to Cloud Insights to complete the configuration of the collector.



For additional information about using Cloud Insights, refer to [Cloud Insights Cloud Agent documentation](#).

Tier data to cloud

Storing data in tiers can enhance the efficiency of your storage system. You can manage

storage tiers by using FabricPool to store data in a tier, based on how frequently the data is accessed.

This procedure sets up an object store as the cloud tier for FabricPool. Keep in mind that once you attach to a local tier (aggr) the cloud tier cannot be unattached.

A FabricPool license is not required when using StorageGRID or ONTAP S3 as the cloud tier or when using Amazon S3, Google Cloud Storage, or Microsoft Azure Blob Storage as the cloud tier for Cloud Volumes for ONTAP. A FabricPool license is required for other cloud tier locations.

If you are tiering to ONTAP S3, there are additional requirements:

- * There must be an entry for the remote ONTAP S3 server's hostname in the DNS server configured for the admin storage VM, including the S3 server's FQDN name and the IP addresses on its network interfaces.

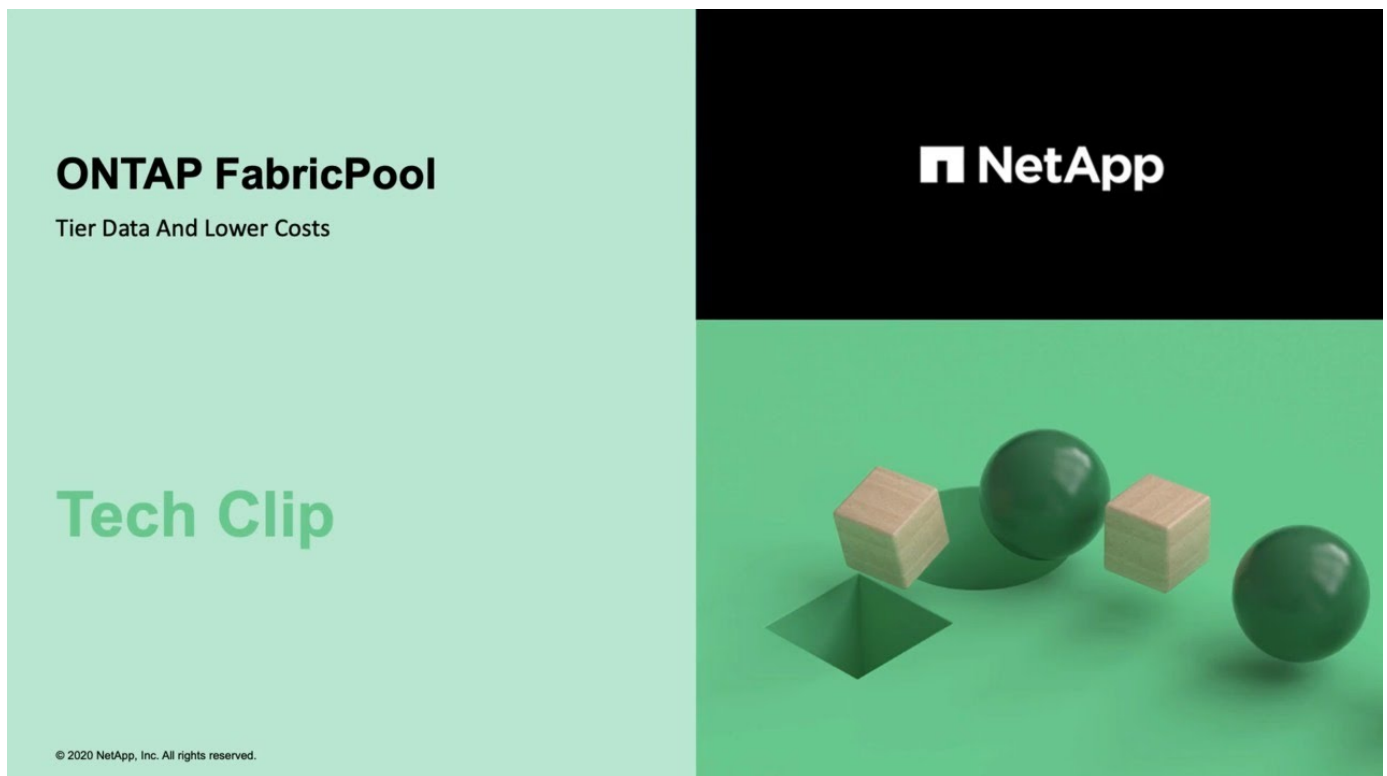
- * [Intercluster network interfaces](#) must be configured on both local and remote clusters, although cluster peering is not required.

You also have the option to create a volume tiering policy in System Manager.

Steps

1. Click **Storage > Tiers > Add Cloud Tier** and select the object store provider you want to use.
2. If you want to create a cloud mirror, click **Add as FabricPool Mirror**.

A FabricPool mirror provides a method for you to seamlessly replace a data store, and it helps to ensure that your data is available in the event of disaster.



Tier data to local bucket


Beginning with ONTAP 9.8, you can tier data to local object storage using ONTAP S3.

Tiering data to a local bucket provides a simple alternative to moving data to a different local tier. This procedure uses an existing bucket on the local cluster, or you can let ONTAP automatically create a new storage VM and a new bucket.

Keep in mind that once you attach to a local tier (aggr) the cloud tier cannot be unattached.

An S3 license is required for this workflow, which creates a new S3 server and new bucket, or uses existing ones. A FabricPool license is not required for this workflow.

Step

1. Tier data to a local bucket: click **Tiers**, select a tier, then click .
 - You have the option to create a new tier (ONTAP S3) or use an existing one.
 - You have the option to edit an existing volume tiering policy.

Create tags for tiering objects

Starting in ONTAP 9.8, you can create object tags to help you classify and sort tiering objects for easier data management. You can set tags only on FabricPool volumes attached to StorageGRID. These tags are retained during a volume move.

Steps


1. Navigate to **Storage > Tiers > Volumes**.
2. Locate the volume you want to tag and select **Click to enter tags**.

Enable inactive data reporting

Starting in ONTAP 9.8, you can enable inactive data reporting to show how much inactive data can be tiered to the cloud.

You can enable inactive data reporting on HDD aggregates.

Steps

1. Choose one of the following options:
 - When you have existing HDD aggregates, navigate to **Storage > Tiers** and click  for the aggregate on which you want to enable inactive data reporting.
 - When no cloud tiers are configured, navigate to **Dashboard** and click the **Enable inactive data reporting** link under **Capacity**.

Back up data using the Cloud Backup Service

Starting with ONTAP 9.9.1, you can use System Manager to back up data in the cloud using Cloud Backup Service.



Cloud Backup Service supports FlexVol read-write volumes and data-protection (DP) volumes. FlexGroup volumes and SnapLock volumes are not supported.

Before you begin

You should perform the following procedures to establish an account in Cloud Manager. For the service

account, you need to create the role as "Account Admin". (Other service account roles do not have the required privileges needed to establish a connection from System Manager.)

1. [Create an account in Cloud Manager](#).
2. [Create a connector in Cloud Manager](#) with one of the following cloud providers:
 - Microsoft Azure
 - Amazon Web Services (AWS)
 - Google Cloud Platform (GCP)
3. [Subscribe to Cloud Backup Service in Cloud Manager](#) (requires the appropriate license).
4. [Generate an access key and a secret key using Cloud Manager](#).

Register the cluster with Cloud Manager

You can register the cluster with Cloud Manager by using either Cloud Manager or System Manager.

Steps

1. In System Manager, go to **Protection Overview**.
2. Under **Cloud Backup Service**, provide the following details:
 - Client ID
 - Client secret key
3. Select **Register and Continue**.

Enable the Cloud Backup Service

After the cluster is registered with Cloud Manager, you can enable the Cloud Backup Service and initiate the first backup to the cloud.

Steps

1. On the **Enable Cloud Backup Service** page, provide the following details:
 - Protection policy (an existing or new policy)
 - Cluster IP space
2. Select the checkbox if you want to back up all volumes in the cluster.
3. Select **Enable**.
4. Depending on which Cloud provider you specified, you need to provide specific information, as follows:

For this cloud provider...	Enter the following data...
Azure	<ul style="list-style-type: none">• Azure Subscription ID• Resource group name (existing or new)• Region• IPspace

For this cloud provider...	Enter the following data...
AWS	<ul style="list-style-type: none"> • AWS Account ID • Access key • Secret key • Region • IPspace
Google Cloud Project (GCP)	<ul style="list-style-type: none"> • Google Cloud Project name • Google Cloud Access key • Google Cloud Secret key • Region • IPspace

Protect new volumes or LUNs on the cloud

When you create a new volume or LUN, you can establish a SnapMirror protection relationship that enables backing up to the cloud for the volume or LUN.

Before you begin

- You should have a SnapMirror license.
- The WORM feature should be disabled.
- Intercluster LIFs should be configured.
- NTP should be configured.
- Cluster must be running ONTAP 9.9.1.
- You cannot use the feature for the following cluster configurations:
 - The cluster cannot be in a MetroCluster environment.
 - SVM-DR is not supported.
 - FlexGroups cannot be backed up using the Cloud Backup Service.

Steps

1. When provisioning a volume or LUN, on the **Protection** page, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
2. Select **Enable Cloud Backup Service**.

Protect existing volumes or LUNs on the cloud

You can establish a SnapMirror protection relationship for existing volumes and LUNs.

Steps

1. Select an existing volume or LUN, and click **Protect**.
2. On the **Protect Volumes** page, specify "Backup using Cloud Backup Service" for the protection policy.

3. Click **Protect**.
4. On the **Protection** page, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
5. Select **Enable Cloud Backup Service**.

Restore data from backup files

You can perform backup management operations, such as restoring data, updating relationships, and deleting relationships, only with Cloud Manager. Refer to [Restoring data from backup files](#) for more information.

Manage the connection to the Cloud Backup Service

Starting with ONTAP 9.9.1, you can use System Manager to back up data in the cloud using the Cloud Backup Service. You can manage the connection to the Cloud Backup Service and view details about the number and capacity of the volumes that are backed up using the service.

Before you begin

You should establish an account in Cloud Manager. For the service account, you need to create the role as "Account Admin". (Other service account roles do not have the required privileges needed to establish a connection from System Manager.) See [Back up data using the Cloud Backup Service](#) for details.

View the status of the connection to the Cloud Backup Service

You can view various details about the connection to the Cloud Backup Service.


Steps

1. Go to **Protection > Overview**.
2. In the **Cloud Backup Service** section, you can view the following details:
 - Status of the connection.
 - The cloud provider.
 - The cloud manager workspace.
 - The number of backed up volumes.
 - The cloud provider used capacity.
 - The cloud manager connector ID.

Modify the connection with the Cloud Backup Service

You can modify the connection to the Cloud Backup Service.

Steps

1. Go to **Protection > Overview**.
2. In the **Cloud Backup Service** section, click .
3. You can select any of the following modification procedures:
 - **Edit**: Allows you to change the protection policy and the IPspace.
 - **Disable**: Stops all further backup operations to the cloud for the cluster.

- **Unlink:** Removes the management of backups to the cloud provider from ONTAP System Manager. However, backups will continue, and they can be managed using Cloud Manager.

Copyright Information

Copyright © 2021 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.