



# **Set up an object store as the cloud tier for FabricPool**

**ONTAP 9**

NetApp  
August 11, 2022

# Table of Contents

- Set up an object store as the cloud tier for FabricPool ..... 1
  - Set up an object store as the cloud tier for FabricPool ..... 1
  - Specify the StorageGRID configuration information ..... 1
  - Attach StorageGRID as a FabricPool cloud tier (video). .... 2
  - Set up ONTAP S3 as the cloud tier ..... 2
  - Set up Alibaba Cloud Object Storage as the cloud tier ..... 3
  - Set up AWS S3 as the cloud tier ..... 4
  - Set up Google Cloud Storage as the cloud tier ..... 6
  - Set up IBM Cloud Object Storage as the cloud tier ..... 7
  - Set up Azure Blob Storage for the cloud as the cloud tier ..... 7
  - Set up object stores for FabricPool in a MetroCluster configuration ..... 8

# Set up an object store as the cloud tier for FabricPool

## Set up an object store as the cloud tier for FabricPool

Setting up FabricPool involves specifying the configuration information of the object store (StorageGRID, ONTAP S3, Alibaba Cloud Object Storage, AWS S3, Google Cloud Storage Platform, IBM Cloud Object Storage, or Microsoft Azure Blob Storage for the cloud) that you plan to use as the cloud tier for FabricPool.

## Specify the StorageGRID configuration information

If you are running ONTAP 9.2 or later, you can set up StorageGRID as the cloud tier for FabricPool. When tiering data that is accessed by SAN protocols, NetApp recommends using private clouds, like StorageGRID, due to connectivity considerations.

### About this task

Load balancing is enabled for StorageGRID in ONTAP 9.8 and later. When the server's hostname resolves to more than one IP address, ONTAP establishes client connections with all the IP addresses returned (up to a maximum of 16 IP addresses). The IP addresses are picked up in a round-robin method when connections are established.

### Steps

1. Specify the StorageGRID configuration information by using the `storage aggregate object-store config create` command with the `-provider-type SGWS` parameter.

- The `storage aggregate object-store config create` command fails if ONTAP cannot access StorageGRID with the provided information.
- You use the `-access-key` parameter to specify the access key for authorizing requests to the StorageGRID object store.
- You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the StorageGRID object store.
- If the StorageGRID password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in StorageGRID without interruption.

- Setting the `-is-certificate-validation-enabled` parameter to `false` disables certificate checking for StorageGRID.

```
cluster1::> storage aggregate object-store config create
-object-store-name mySGWS -provider-type SGWS -server mySGWSserver
-container-name mySGWScontainer -access-key mySGWSkey
-secret-password mySGWSpass
```

2. Display and verify the StorageGRID configuration information by using the `storage aggregate`

`object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the StorageGRID configuration information for FabricPool.

## Attach StorageGRID as a FabricPool cloud tier (video)

This video shows a quick overview of using System Manager to attach a StorageGRID bucket to ONTAP aggregates with FabricPool.

[NetApp video: Attaching StorageGRID Webscale as a FabricPool external capacity tier](#)

### Related information

[NetApp TechComm TV: FabricPool playlist](#)

## Set up ONTAP S3 as the cloud tier

If you are running ONTAP 9.8 or later, you can set up ONTAP S3 as the cloud tier for FabricPool.

### What you'll need

You must have the ONTAP S3 server name and the IP address of its associated LIFs on the remote cluster.

There must be intercluster LIFs on both local and remote clusters.

[Creating intercluster LIFs for remote FabricPool tiering](#)

### About this task

Load balancing is enabled for ONTAP S3 servers in ONTAP 9.8 and later. When the server's hostname resolves to more than one IP address, ONTAP establishes client connections with all the IP addresses returned (up to a maximum of 16 IP addresses). The IP addresses are picked up in a round-robin method when connections are established.

### Steps

1. Add entries for the S3 server and LIFs to your DNS server.

Option	Description
If you use an external DNS server	Give the S3 server name and IP addresses to the DNS server administrator.
If you use your local system's DNS hosts table	Enter the following command:  <pre>dns host create -vserver svm_name -address ip_address -hostname s3_server_name</pre>

2. Specify the ONTAP S3 configuration information by using the `storage aggregate object-store config create` command with the `-provider-type ONTAP_S3` parameter.

- The `storage aggregate object-store config create` command fails if the local ONTAP system cannot access the ONTAP S3 server with the information provided.
- You use the `-access-key` parameter to specify the access key for authorizing requests to the ONTAP S3 server.
- You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the ONTAP S3 server.
- If the ONTAP S3 server password is changed, you should immediately update the corresponding password stored in the local ONTAP system.

Doing so enables access to the data in the ONTAP S3 object store without interruption.

- Setting the `-is-certificate-validation-enabled` parameter to `false` disables certificate checking for ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server
-container-name myS3container -access-key myS3key
-secret-password myS3pass
```

3. Display and verify the ONTAP\_S3 configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the ONTAP\_S3 configuration information for FabricPool.

## Set up Alibaba Cloud Object Storage as the cloud tier

If you are running ONTAP 9.6 or later, you can set up Alibaba Cloud Object Storage as the cloud tier for FabricPool.

### Steps

1. Specify the Alibaba Cloud Object Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type AliCloud` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access Alibaba Cloud Object Storage with the provided information.
  - You use the `-access-key` parameter to specify the access key for authorizing requests to the Alibaba Cloud Object Storage object store.
  - If the Alibaba Cloud Object Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in Alibaba Cloud Object Storage without interruption.

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Display and verify the Alibaba Cloud Object Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the Alibaba Cloud Object Storage configuration information for FabricPool.

## Set up AWS S3 as the cloud tier

If you are running ONTAP 9.2 or later, you can set up AWS S3 as the cloud tier for FabricPool. If you are running ONTAP 9.5 or later, you can set up AWS Commercial Cloud Services (C2S) for FabricPool.

### Steps

1. Specify the AWS S3 configuration information by using the `storage aggregate object-store config create` command with the `-provider-type AWS_S3` parameter.

- You use the `-auth-type CAP` parameter to obtain credentials for C2S access.

When you use the `-auth-type CAP` parameter, you must use the `-cap-url` parameter to specify the full URL to request temporary credentials for C2S access.

- The `storage aggregate object-store config create` command fails if ONTAP cannot access AWS S3 with the provided information.
- You use the `-access-key` parameter to specify the access key for authorizing requests to the AWS S3 object store.
- You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the AWS S3 object store.
- If the AWS S3 password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in AWS S3 without interruption.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

```
cluster1::> storage aggregate object-store config create -object
-store-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap
-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&r
ole=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-
bucket
```

2. Display and verify the AWS S3 configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the AWS S3 configuration information for FabricPool.

## Set up AWS S3 as the cloud tier

If you are running ONTAP 9.2 or later, you can set up AWS S3 as the cloud tier for FabricPool. If you are running ONTAP 9.5 or later, you can set up AWS Commercial Cloud Services (C2S) for FabricPool.

### Steps

1. Specify the AWS S3 configuration information by using the `storage aggregate object-store config create` command with the `-provider-type AWS_S3` parameter.

- You use the `-auth-type CAP` parameter to obtain credentials for C2S access.

When you use the `-auth-type CAP` parameter, you must use the `-cap-url` parameter to specify the full URL to request temporary credentials for C2S access.

- The `storage aggregate object-store config create` command fails if ONTAP cannot access AWS S3 with the provided information.
- You use the `-access-key` parameter to specify the access key for authorizing requests to the AWS S3 object store.
- You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the AWS S3 object store.
- If the AWS S3 password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in AWS S3 without interruption.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

```
cluster1::> storage aggregate object-store config create -object
-store-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap
-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&r
ole=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-
bucket
```

2. Display and verify the AWS S3 configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the AWS S3 configuration information for FabricPool.

## Attach AWS S3 as a FabricPool cloud tier (video)

This video shows a quick overview of using System Manager to attach an AWS S3 bucket to ONTAP aggregates with FabricPool.

[NetApp video: Attaching Amazon S3 as a FabricPool external capacity tier](#)

### Related information

[NetApp TechComm TV: FabricPool playlist](#)

## Set up Google Cloud Storage as the cloud tier

If you are running ONTAP 9.6 or later, you can set up Google Cloud Storage as the cloud tier for FabricPool.

### Steps

1. Specify the Google Cloud Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type GoogleCloud` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access Google Cloud Storage with the provided information.
  - You use the `-access-key` parameter to specify the access key for authorizing requests to the Google Cloud Storage object store.
  - If the Google Cloud Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in Google Cloud Storage without interruption.

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```



2. Display and verify the Google Cloud Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the Google Cloud Storage configuration information for FabricPool.

## Set up IBM Cloud Object Storage as the cloud tier

If you are running ONTAP 9.5 or later, you can set up IBM Cloud Object Storage as the cloud tier for FabricPool.

### Steps

1. Specify the IBM Cloud Object Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type IBM_COS` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access IBM Cloud Object Storage with the provided information.
  - You use the `-access-key` parameter to specify the access key for authorizing requests to the IBM Cloud Object Storage object store.
  - You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the IBM Cloud Object Storage object store.
  - If the IBM Cloud Object Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in IBM Cloud Object Storage without interruption.

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Display and verify the IBM Cloud Object Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the IBM Cloud Object Storage configuration information for FabricPool.

## Set up Azure Blob Storage for the cloud as the cloud tier

If you are running ONTAP 9.4 or later, you can set up Azure Blob Storage for the cloud as the cloud tier for FabricPool.

### About this task

FabricPool currently does not support Azure Stack, which is on-premises Azure services.

### Steps

1. Specify the Azure Blob Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type Azure_Cloud` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access Azure Blob Storage with the provided information.
  - You use the `-azure-account` parameter to specify the Azure Blob Storage account.
  - You use the `-azure-private-key` parameter to specify the access key for authenticating requests to Azure Blob Storage.
  - If the Azure Blob Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in Azure Blob Storage without interruption.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyAzure -provider-type Azure_Cloud
-server blob.core.windows.net -container-name myAzureContainer
-azure-account myAzureAcct -azure-private-key myAzureKey
```

2. Display and verify the Azure Blob Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the Azure Blob Storage configuration information for FabricPool.

## Set up object stores for FabricPool in a MetroCluster configuration

If you are running ONTAP 9.7 or later, you can set up a mirrored FabricPool on a MetroCluster configuration to tier cold data to object stores in two different fault zones.

### What you'll need

- The MetroCluster configuration is set up and properly configured.
- Two object stores are set up on the appropriate MetroCluster sites.
- Containers are configured on each of the object stores.
- IP spaces are created or identified on the two MetroCluster configurations and their names match.

### About this task

- FabricPool in MetroCluster requires that the underlying mirrored aggregate and the associated object store configuration must be owned by the same MetroCluster configuration.
- You cannot attach an aggregate to an object store that is created in the remote MetroCluster site.
- You must create object store configurations on the MetroCluster configuration that owns the aggregate.

### Step

1. Specify the object store configuration information on each MetroCluster site by using the `storage object-store config create` command.

In this example, FabricPool is required on only one cluster in the MetroCluster configuration. Two object store configurations are created for that cluster, one for each object store bucket.

```
storage aggregate
  object-store config create -object-store-name mcc1-ostore-config-s1
-provider-type SGWS -server
  <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
-secret-password <password> -encrypt
  <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
  <IPSpace>
```

```
storage aggregate object-store config create -object-store-name mcc1-
ostore-config-s2
  -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
bucket-2> -access-key <key> -secret-password <password> -encrypt
<true|false> -provider <provider-type>
  -is-ssl-enabled <true|false> ipspace <IPSpace>
```

This example sets up FabricPool on the second cluster in the MetroCluster configuration.

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s1
-provider-type SGWS -server
  <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
-secret-password <password> -encrypt
  <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
  <IPSpace>
```

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s2
-provider-type SGWS -server
  <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
-secret-password <password> -encrypt
  <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
  <IPSpace>
```

## 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.