# Prepare for FabricPool configuration

ONTAP 9

NetApp
July 20, 2022

# Table of Contents

# Prepare for FabricPool configuration

## Prepare for FabricPool configuration overview

Configuring FabricPool helps you manage which storage tier (the local performance tier or the cloud tier) data should be stored based on whether the data is frequently accessed.

The preparation required for FabricPool configuration depends on the object store you use as the cloud tier.

## Install a FabricPool license

Newly ordered AFF systems come with a free 10 TB capacity term-based license for using non-NetApp object stores (AWS S3, Azure Blob Storage, IBM Cloud Object Storage, Alibaba Cloud Object Storage, or Google Cloud Storage) with FabricPool, if you select it. If you need additional capacity on an AFF system, if you plan to use non-NetApp object stores with a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

**About this task**

The FabricPool license is a cluster-wide license. It includes an entitled usage limit that you purchase for the AWS S3, Azure Blob Storage, or IBM Cloud Object Storage, Alibaba Cloud Object Storage, or Google Cloud Storage cloud tier that is associated with FabricPool in the cluster. The usage across the cluster must not exceed the capacity of the entitled usage limit. If you need to increase the usage limit of the license, you should contact your sales representative.

FabricPool licenses are available in perpetual or term-based, 1- or 3- year, formats.

A term-based FabricPool license with 10 TB of free capacity is available for first time FabricPool orders for existing clusters. Free capacity is not available with perpetual licenses.

A license is not required if you use NetApp StorageGRID or ONTAP S3 for the cloud tier. Cloud Volumes ONTAP does not require a FabricPool license, regardless of the provider you are using.

This task is supported only by uploading the license file to the cluster using System Manager.

**Steps**

1. Download the NetApp License File (NLF) for the FabricPool license from the NetApp Support Site.

   NetApp Support

2. Use System Manager to upload the FabricPool license to the cluster:
   a. Depending on the ONTAP release running on your storage system, perform the following action:

| If you are running… | Perform the following action: |
| --- | --- |
| ONTAP 9.4 or earlier | Click **Configuration** > **Licenses**. |

| | |
|---|---|
| ONTAP 9.5 or later | Click **Configuration** > **Cluster** > **Licenses**. |

b. In the **Cluster Settings** pane, click **Licenses**.

c. In the **Packages** window, click **Add**.

d. In the **Add License Packages** dialog box, click **Choose Files** to select the NLF you downloaded, and then click **Add** to upload the file to the cluster.

**Related information**

ONTAP FabricPool (FP) Licensing Overview

NetApp Software License Search

# Install a FabricPool license (video)

This video shows a quick overview of using System Manager to install a FabricPool license for non-NetApp object stores such as AWS S3.

NetApp video: Installing a FabricPool license

**Related information**

NetApp TechComm TV: FabricPool playlist

# Install a CA certificate if you use StorageGRID

Unless you plan to disable certificate checking for StorageGRID, you must install a StorageGRID CA certificate on the cluster so that ONTAP can authenticate with StorageGRID as the object store for FabricPool.

**About this task**

ONTAP 9.4 and later releases enable you to disable certificate checking for StorageGRID.

**Steps**

1. Contact your StorageGRID administrator to obtain the StorageGRID system's CA certificate.
2. Use the `security certificate install` command with the `-type server-ca` parameter to install the StorageGRID CA certificate on the cluster.

   The fully qualified domain name (FQDN) you enter must match the custom common name on the StorageGRID CA certificate.

## Update an expired certificate

To update an expired certificate, the best practice is to use a trusted CA to generate the new server certificate. In addition, you should ensure that the certificate is updated on the StorageGRID server and on the ONTAP cluster at the same time to keep any downtime to a minimum.

**Related information**

StorageGRID Resources

# Install a CA certificate if you use ONTAP S3

Unless you plan to disable certificate checking for ONTAP S3, you must install a ONTAP S3 CA certificate on the cluster so that ONTAP can authenticate with ONTAP S3 as the object store for FabricPool.

**Steps**

1. Obtain the ONTAP S3 system's CA certificate.
2. Use the `security certificate install` command with the `-type server-ca` parameter to install the ONTAP S3 CA certificate on the cluster.

   The fully qualified domain name (FQDN) you enter must match the custom common name on the ONTAP S3 CA certificate.

## Update an expired certificate

To update an expired certificate, the best practice is to use a trusted CA to generate the new server certificate. In addition, you should ensure that the certificate is updated on the ONTAP S3 server and on the ONTAP cluster at the same time to keep any downtime to a minimum.

**Related information**

S3 configuration

# 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:<br><br>`dns host create -vserver svm_name -address ip_address -hostname s3_server_name` |

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 objects 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>
```

# Attach the cloud tier to an aggregate

After setting up an object store as the cloud tier, you specify the aggregate to use by attaching it to FabricPool. In ONTAP 9.5 and later, you can also attach aggregates that contain qualified FlexGroup volume constituents.

**What you'll need**

When you use the ONTAP CLI to set up an aggregate for FabricPool, the aggregate must already exist.

When you use System Manager to set up an aggregate for FabricPool, you can create the aggregate and set it up to use for FabricPool at the same time.

**Steps**

1. **Optional**: To see how much data in a volume is inactive, follow the steps in Determining how much data in a volume is inactive by using inactive data reporting.

   Seeing how much data in a volume is inactive can help you decide which aggregate to use for FabricPool.

2. Attach the object store to an aggregate by using the `storage aggregate object-store attach` command.

   If the aggregate has never been used with FabricPool and it contains existing volumes, then the volumes are assigned the default `snapshot-only` tiering policy.

   ```
   cluster1::> storage aggregate object-store attach -aggregate myaggr
   -object-store-name Amazon01B1
   ```

   You can use the `allow-flexgroup true` option to attach aggregates that contain FlexGroup volume constituents.

3. Display the object store information and verify that the attached object store is available by using the `storage aggregate object-store show` command.

```
cluster1::> storage aggregate object-store show

Aggregate    Object Store Name    Availability State
---------    -----------------    ------------------
myaggr       Amazon01B1           available
```