Prepare for FabricPool configuration

ONTAP 9

NetApp
February 07, 2023

This PDF was generated from https://docs.netapp.com/us-en/ontap/fabricpool/prepare-config-task.html on February 07, 2023. Always check docs.netapp.com for the latest.

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.

Add a connection to the cloud

Beginning 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.

> If you choose the option to use a proxy server when adding a connection from Cloud Volumes ONTAP to Cloud Insights Service, you must ensure that the URL https://example.com is accessible from the proxy server. The message "The HTTP Proxy configuration is not valid" is displayed when https://example.com is not accessible.

Steps

1. In Cloud Insights, during the process to configure a collector, copy the generated pairing code.
2. Using System Manager with ONTAP 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. Select **Add**.
7. Return to Cloud Insights to complete the configuration of the collector.

For additional information about Cloud Insights, refer to Cloud Insights documentation.

Install a FabricPool license

The FabricPool license you might have used in the past is changing and is being retained only for configurations that aren’t supported within BlueXP. Starting August 21, 2021, new Cloud Tiering BYOL licensing was introduced for tiering configurations that are supported within BlueXP using the Cloud Tiering service.

Learn more about the new Cloud Tiering BYOL licensing.

Configurations that are supported by BlueXP must use the Digital Wallet page in BlueXP to license tiering for

ONTAP clusters. This requires you to set up a BlueXP account and set up tiering for the particular object storage provider you plan to use. BlueXP currently supports tiering to the following object storage: Amazon S3, Azure Blob storage, Google Cloud Storage, S3-compatible object storage, and StorageGRID.

Learn more about the Cloud tiering service.

You can download and activate a FabricPool license using System Manager if you have one of the configurations that is not supported within BlueXP:

- ONTAP installations in Dark Sites
- ONTAP clusters that are tiering data to IBM Cloud Object Storage or Alibaba Cloud Object Storage

The FabricPool license is a cluster-wide license. It includes an entitled usage limit that you purchase for object storage 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 configurations not supported within BlueXP. 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.
2. Perform the following actions using System Manager to upload the FabricPool license to the cluster:
   a. In the **Cluster > Settings** pane, on the **Licenses** card, click →.
   b. On the **License** page, click + Add .
   c. In the **Add License** dialog box, click **Browse** 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

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 overview

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.

Set up StorageGRID as the cloud tier

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.

Considerations for using StorageGRID with FabricPool

- You need to install a CA certificate for StorageGRID, unless you explicitly disable certificate checking.
- You must not enable StorageGRID object versioning on the object store bucket.
- A FabricPool license is not required.
- If a StorageGRID node is deployed in a virtual machine with storage assigned from a NetApp AFF system, confirm that the volume does not have a FabricPool tiering policy enabled.

  Disabling FabricPool tiering for volumes used with StorageGRID nodes simplifies troubleshooting and storage operations.

> Never use FabricPool to tier any data related to StorageGRID back to StorageGRID itself. Tiering StorageGRID data back to StorageGRID increases troubleshooting and operational complexity.

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.

Procedures

You can set up StorageGRID as the cloud tier for FabricPool with ONTAP System Manager or the ONTAP CLI.

System Manager

1. Click **Storage > Tiers > Add Cloud Tier** and select StorageGRID as the object store provider.
2. Complete the requested information.
3. 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.

CLI

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.

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 the local cluster.

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.

Procedures

You can set up ONTAP S3 as the cloud tier for FabricPool with ONTAP System Manager or the ONTAP CLI.

System Manager

1. Click **Storage > Tiers > Add Cloud Tier** and select ONTAP S3 as the object store provider.
2. Complete the requested information.
3. 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.

CLI

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: `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.

Considerations for using Alibaba Cloud Object Storage with FabricPool

- You might need a FabricPool license.

  Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use Alibaba Cloud Object Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Alibaba Object Storage Service classes:
  - Alibaba Object Storage Service Standard
  - Alibaba Object Storage Service Infrequent Access

    Alibaba Cloud: Introduction to storage classes

Contact your NetApp sales representative for information about storage classes not listed.

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.

Considerations for using AWS S3 with FabricPool

- You might need a FabricPool license.
  - Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool.

    If you need additional capacity on an AFF system, if you use AWS S3 on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

    If you order FabricPool for the first time for an existing cluster, a FabricPool license with 10 TB of free capacity is available.
- The LIF that ONTAP uses to connect with the AWS S3 object server must be on a 10 Gbps port.
- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Amazon S3 storage classes:
  - Amazon S3 Standard
  - Amazon S3 Standard - Infrequent Access (Standard - IA)
  - Amazon S3 One Zone - Infrequent Access (One Zone - IA)
  - Amazon S3 Intelligent-Tiering
  - Amazon Commercial Cloud Services

    Amazon Web Services (AWS) Documentation: Amazon S3 Storage Classes

  Contact your sales representative for information about storage classes not listed.
- On Cloud Volumes ONTAP, FabricPool supports tiering from General Purpose SSD (gp2) and Throughput Optimized HDD (st1) volumes of Amazon Elastic Block Store (EBS).

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.

Considerations for using AWS S3 with FabricPool

- You might need a FabricPool license.
  - Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool.

    If you need additional capacity on an AFF system, if you use AWS S3 on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

    If you order FabricPool for the first time for an existing cluster, a FabricPool license with 10 TB of free capacity is available.
- The LIF that ONTAP uses to connect with the AWS S3 object server must be on a 10 Gbps port.
- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Amazon S3 storage classes:
  - Amazon S3 Standard
  - Amazon S3 Standard - Infrequent Access (Standard - IA)
  - Amazon S3 One Zone - Infrequent Access (One Zone - IA)
  - Amazon S3 Intelligent-Tiering
  - Amazon Commercial Cloud Services

Amazon Web Services (AWS) Documentation: Amazon S3 Storage Classes

Contact your sales representative for information about storage classes not listed.

- On Cloud Volumes ONTAP, FabricPool supports tiering from General Purpose SSD (gp2) and Throughput Optimized HDD (st1) volumes of Amazon Elastic Block Store (EBS).

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 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.

Additional considerations for using Google Cloud Storage with FabricPool

- You might need a FabricPool license.

  Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use Google Cloud Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

- The LIF that ONTAP uses to connect with the Google Cloud Storage object server must be on a 10 Gbps port.
- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Google Cloud Object storage classes:
  - Google Cloud Multi-Regional
  - Google Cloud Regional
  - Google Cloud Nearline
  - Google Cloud Coldline

    Google Cloud: Storage Classes

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.

Considerations for using IBM Cloud Object Storage with FabricPool

- You might need a FabricPool license.

  Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use IBM Cloud Object Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

  If you order FabricPool for the first time for an existing cluster, a FabricPool license with 10 TB of free capacity is available.

- The LIF that ONTAP uses to connect with the IBM Cloud object server must be on a 10 Gbps port.

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.

Considerations for using Microsoft Azure Blob Storage with FabricPool

- You might need a FabricPool license.

  Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use Azure Blob Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

  If you order FabricPool for the first time for an existing cluster, a FabricPool license with 10 TB of free capacity is available.

- A FabricPool license is not required if you are using Azure Blob Storage with Cloud Volumes ONTAP.
- The LIF that ONTAP uses to connect with the Azure Blob Storage object server must be on a 10 Gbps port.
- FabricPool currently does not support Azure Stack, which is on-premises Azure services.
- At the account level in Microsoft Azure Blob Storage, FabricPool supports only hot and cool storage tiers.

  FabricPool does not support blob-level tiering. It also does not support tiering to Azure's archive storage tier.

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 a local tier (aggregate)

After setting up an object store as the cloud tier, you specify the local tier (aggregate) to use by attaching it to FabricPool. In ONTAP 9.5 and later, you can also attach local tiers (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 a local tier for FabricPool, you can create the local tier and set it up to use for FabricPool at the same time.

Procedures

You can attach a local tier (aggregate) to a FabricPool object store with ONTAP System Manager or the ONTAP CLI.

System Manager

1. Navigate to **Storage > Tiers**, select a cloud tier, then click ⋮.
2. Select **Attach local tiers**.
3. Under **Add as Primary** verify that the volumes are eligible to attach.
4. If necessary, select **Convert volumes to thin provisioned**.
5. Click **Save**.

CLI

To attach an object store to an aggregate with the CLI:

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
   ```

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 (aggregate) 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 ⋮.
2. If necessary, enable thin provisioning.
3. Choose an existing tier or create a new one.
4. If necessary, edit the existing tiering policy.

Copyright information

Copyright © 2023 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.