Abstract

This technical report describes best practices for the NetApp® ONTAP® software component FabricPool. The capabilities, requirements, implementation, and best practices for this software are covered.
# TABLE OF CONTENTS

1 Overview ........................................................................................................................................... 4

2 Primary Use Cases .......................................................................................................................... 5
   2.1 Reclaim Capacity on Primary Storage (Auto, Snapshot-Only, or All) ....................................... 5
   2.2 Shrink the Secondary Storage Footprint (All) ........................................................................... 8

3 Requirements ..................................................................................................................................... 9
   3.1 Platforms ...................................................................................................................................... 9
   3.2 Intercluster LIFs ......................................................................................................................... 9
   3.3 Volumes ..................................................................................................................................... 10
   3.4 FabricPool License ................................................................................................................... 10
   3.5 Certificate Authority Certification .......................................................................................... 13

4 Architecture ....................................................................................................................................... 14
   4.1 Block Temperature ..................................................................................................................... 14
   4.2 Object Creation .......................................................................................................................... 14
   4.3 Data Movement .......................................................................................................................... 14
   4.4 Object Storage .......................................................................................................................... 19

5 Configuration ...................................................................................................................................... 21
   5.1 Create a Bucket/Container ....................................................................................................... 21
   5.2 Add a Cloud Tier to ONTAP .................................................................................................... 23
   5.3 Attach a Cloud Tier to a Local Tier ......................................................................................... 26
   5.4 Set Volume Tiering Policies ..................................................................................................... 28
   5.5 Set Volume Tiering Minimum Cooling Days ........................................................................... 30
   5.6 FabricPool Mirror .................................................................................................................... 31
   5.7 MetroCluster ............................................................................................................................. 35
   5.8 Security ..................................................................................................................................... 36

6 Interoperability .................................................................................................................................. 37
   6.1 StorageGRID ............................................................................................................................. 38

7 Performance ....................................................................................................................................... 40
   7.1 Sizing the Local Tier ................................................................................................................ 40
   7.2 Sizing the Cloud Tier ................................................................................................................. 40
   7.3 Connectivity ............................................................................................................................... 42
   7.4 Capacity ..................................................................................................................................... 44
   7.5 Virtualized Object Storage ....................................................................................................... 46
1 Overview

FabricPool, first available in ONTAP 9.2, is a NetApp Data Fabric technology that enables automated tiering of data to low-cost object storage tiers either on or off premises.

Unlike manual tiering solutions, FabricPool reduces total cost of ownership by automating the tiering of data to lower the cost of storage. It delivers the benefits of cloud economics by tiering to public clouds such as Alibaba Cloud Object Storage Service, Amazon S3, Google Cloud Storage, IBM Cloud Object Storage, and Microsoft Azure Blob Storage as well as to private clouds such as NetApp StorageGRID®.

FabricPool is transparent to applications and allows enterprises to take advantage of cloud economics without sacrificing performance or having to rearchitect solutions to leverage storage efficiency.

- ONTAP supports FabricPool on NetApp AFF systems and all-SSD local tiers (also known as storage aggregates in the ONTAP CLI) on FAS systems.
- Cloud Volumes ONTAP supports data tiering with Amazon S3, Google Cloud Storage, and Microsoft Azure Blob Storage.

Figure 1) Before and after FabricPool.
2 Primary Use Cases

The primary purpose of FabricPool is to reduce storage footprints and associated costs. Active data remains on high-performance SSDs and inactive data is tiered to low-cost object storage while preserving ONTAP functionality and data efficiencies.

FabricPool has two primary use cases:

- Reclaim capacity on primary storage
- Shrink the secondary storage footprint

Although FabricPool can significantly reduce storage footprints in primary and secondary data centers, it is not a backup solution. Access control lists (ACLs), directory structures, and NetApp WAFL® metadata always stays on the local tier. If a catastrophic disaster destroys the local tier, a new environment cannot be created using the data on the cloud tier because it contains no WAFL metadata.

For complete data protection, consider using existing ONTAP technologies such as NetApp SnapMirror® and NetApp SnapVault®.

2.1 Reclaim Capacity on Primary Storage (Auto, Snapshot-Only, or All)

Auto

The majority of inactive (cold) data in storage environments is associated with unstructured data, accounting for more than 50% of total storage capacity in many storage environments.

Infrequently accessed data associated with productivity software, completed projects, and old datasets is an inefficient use of high-performance SSDs, and tiering this data to a low-cost object store is an easy way to reclaim existing SSD capacity and reduce the amount of required SSD capacity moving forward.

First available in ONTAP 9.4, the Auto volume tiering policy, shown in Figure 2, moves all cold blocks in the volume, not just blocks associated with NetApp Snapshot™ copies, to the cloud tier.

If read by random reads, cold data blocks on the cloud tier become hot and are moved to the local tier. If read by sequential reads such as those associated with index and antivirus scans, cold data blocks on the cloud tier stay cold and are not written to the local tier.

Figure 2) Reclaiming space with the auto-volume tiering policy.
**Snapshot-Only**

Snapshot copies can frequently consume more than 10% of a typical storage environment. Although essential for data protection and disaster recovery, these point-in-time copies are rarely used and are an inefficient use of high-performance SSDs.

Snapshot-Only, a volume tiering policy for FabricPool, is an easy way to reclaim storage space on SSDs. When configured to use this policy, cold Snapshot blocks in the volume that are not shared with the active file system are moved to the cloud tier. If read, cold data blocks on the cloud tier become hot and are moved to the local tier.

**Note:** The FabricPool Snapshot-Only volume tiering policy, as shown in Figure 3, reduces the amount of storage used by Snapshot copies on SSDs. It does not increase the maximum number of Snapshot copies allowed by ONTAP, which remains 1,023.

**Figure 3**) Reclaiming space with the Snapshot-Only volume tiering policy.
All

In addition to cold primary data in active volumes (Auto) and snapshots (Snapshot-Only), one of the most common uses of FabricPool is to move entire volumes of data to low-cost clouds. Completed projects, legacy reports, or historical records—any dataset that must be retained but is unlikely to be frequently read—are ideal candidates to be tiered to low-cost object storage.

Moving entire volumes is accomplished by setting the All volume tiering policy on a volume. The All volume tiering policy, as shown in Figure 4, is primarily used with secondary data and data protection volumes, but it can be also be used to tier all data in read/write volumes, provided the volume is not subject to frequent transactional operations.

Data in volumes using the All tiering policy, (excluding data illegible for tiering) is immediately marked as cold and tiered to the cloud as soon as possible. There is no waiting for a minimum number of days to pass before the data is made cold and tiered. If read, cold data blocks on the cloud tier stay cold and are not written back to the local tier.

Figure 4) Reclaiming space with the All volume tiering policy.
2.2 Shrink the Secondary Storage Footprint (All)

Secondary data includes data protection volumes that are NetApp SnapMirror (disaster recovery) or NetApp SnapVault (backup) destination targets. This data is frequently stored on secondary clusters that share a 1:1 or greater ratio with the primary data that they are protecting (one baseline copy and multiple Snapshot copies). For large datasets, this approach can be prohibitively expensive, forcing users to make expensive decisions about the data they need to protect.

Like Snapshot copies, data protection volumes are infrequently used, are an inefficient use of high-performance SSDs, and are expensive for large datasets even when using HDDs. FabricPool’s All volume tiering policy changes this paradigm.

Instead of 1:1 primary-to-backup ratios, the FabricPool All policy allows users to significantly reduce the number of disk shelves on their secondary clusters, tiering most of the backup data to low-cost object stores. ACLs, directory structures, and WAFL metadata remains on the secondary cluster’s local tier.

If read, cold data blocks in volumes using the All policy are not written back to the local tier. This reduces the need for high-capacity secondary storage local tiers.

Figure 5) Using the All volume tiering policy with secondary storage.

Figure 5 illustrates the secondary as a traditional cluster running ONTAP. The secondary can also be in the cloud using Cloud ONTAP Volumes, or in a software defined environment using ONTAP Select. Data can be tiered using FabricPool anywhere ONTAP can be deployed.
3 Requirements

FabricPool requires ONTAP 9.2 or later and the use of SSD local tiers on any of the platforms listed in the next section. Additional FabricPool requirements depend on the cloud tier being attached.

Although installation and use of certificate authority (CA) certificates are recommended best practices, starting in ONTAP 9.4, installation of CA certificates is not required for StorageGRID.

3.1 Platforms

FabricPool is supported on all platforms capable of running ONTAP 9.2 except for the following:

- **FAS**
  - FAS8020
  - FAS2554, FAS2552, FAS2520
  **Note:** Only SSD local tiers on FAS platforms can use FabricPool.

- **ONTAP Select**
  **Note:** NetApp recommends using all-SSD FabricPool local tiers.

- **Cloud tiers**
  - Alibaba Cloud Object Storage Service (Standard, Infrequent Access)
  - Amazon S3 (Standard, Standard-IA, One Zone-IA, Intelligent-Tiering)
  - Amazon Commercial Cloud Services (C2S)
  - Google Cloud Storage (Multi-Regional, Regional, Nearline, Coldline, Archive)
  - IBM Cloud Object Storage (Standard, Vault, Cold Vault, Flex)
  - Microsoft Azure Blob Storage (Hot and Cool)
  - StorageGRID 10.3+

- **Data Tiering with Cloud Volumes ONTAP**
  - Amazon S3
  - Google Cloud Storage
  - Microsoft Azure Blob Storage

3.2 Intercluster LIFs

Cluster high-availability (HA) pairs that use FabricPool require two intercluster LIFs to communicate with the cloud tier. NetApp recommends creating an intercluster LIF on additional HA pairs to seamlessly attach cloud tiers to local tiers on those nodes as well.

If you are using more than one IC LIF on a node with different routing, NetApp recommends placing them in different IPspaces. During configuration, FabricPool can select from multiple IPspaces, but it is unable to select specific IC LIFs within an IPspace.

**Note:** Disabling or deleting an intercluster LIF interrupts communication to the cloud tier.
3.3 Volumes

FabricPool cannot attach a cloud tier to an local tier that contains volumes using a space guarantee other than None (for example, Volume).

```
volume modify -space-guarantee none
```

Setting the `space-guarantee none` parameter assures thin provisioning of the volume. The amount of space consumed by volumes with this guarantee type grows as data is added instead of being determined by the initial volume size. This approach is essential for FabricPool because the volume must support cloud tier data that becomes hot and is brought back to the local tier.

### FlexGroup Volumes

All local tiers used by a NetApp FlexGroup volume must be FabricPool local tiers.

When provisioning FlexGroup volumes on FabricPool local tiers, automatic processes in ONTAP System Manager (formerly OnCommand® System Manager) require that the FlexGroup volume uses FabricPool local tiers on every cluster node. This is a recommended best practice but is not a requirement when manually provisioning FlexGroup volumes.

### Quality of Service Minimums

FabricPool and quality of service minimums (QoS Min) goals are mutually exclusive; QoS Min provides performance minimums, whereas FabricPool sends blocks to an object store—decreasing performance. QoS Min must be turned off on volumes in FabricPool local tiers. Alternatively, tiering must be turned off (`-tiering-policy none`) on volumes that need QoS Min.

3.4 FabricPool License

FabricPool requires a capacity-based license when attaching third-party object storage providers (such as Amazon S3) as cloud tiers for AFF and FAS hybrid flash systems. A FabricPool license is not required when using StorageGRID 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.

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

Tiering to the cloud tier stops when the amount of data (used capacity) stored on the cloud tier reaches the licensed capacity. Additional data, including SnapMirror copies to volumes using the All tiering policy, cannot be tiered until the license capacity is increased. Although tiering stops, data remains accessible from the cloud tier. Additional cold data remains on SSDs until the licensed capacity is increased.

A free 10TB capacity, term-based FabricPool license comes with the purchase of any new ONTAP 9.5+ cluster, although additional support costs might apply. FabricPool licenses (including additional capacity for existing licenses) can be purchased in 1TB increments.

A FabricPool license can only be deleted from a cluster containing no FabricPool local tiers.

**Note:** FabricPool licenses are cluster wide. Have your UUID available when purchasing a license (`cluster identity show`). For additional licensing information, refer to the [NetApp Knowledgebase](https://www.netapp.com/en-us/home/).
Installation

After you acquire a NetApp license file (NLF), you can install it by using ONTAP System Manager. To do so, complete the following steps:

1. Click CLUSTER.
2. Click Settings.
3. Click Licenses.
4. Click Add.
5. Click Choose Files to browse and select a file.
6. Click Add.

Figure 6) FabricPool license.
License Capacity

Licensed capacity can be viewed using the ONTAP CLI as well as ONTAP System Manager. To view the licensed capacity, run the following command in the ONTAP CLI:

```
system license show-status
```

In ONTAP System Manager, complete the following steps:

1. Click CLUSTER.
2. Click Settings.
3. Click Licenses.
4. Click the FabricPool License.
5. Click the down arrow to view license details.

Maximum capacity and current capacity are listed on the FabricPool License row.

Figure 7) License capacity.
3.5 Certificate Authority Certification

When FabricPool uses StorageGRID or other private clouds like some IBM Cloud Object Storage environments as a cloud tier, it must use a Transport Layer Security (TLS) connection. Using FabricPool without TLS configuration is supported but not recommended.

Note: Starting in ONTAP 9.4, CA certificates are no longer required. However, using signed certificates from a third-party certificate authority remains the recommended best practice.

FQDN

FabricPool requires that CA certificates use the same fully qualified domain name (FQDN) as the cloud tier server with which they are associated.

Prior to StorageGRID 11.3, the default CA certificates use a common name (CN) that isn’t based on the server’s FQDN. Using the common name will causes certificate-based errors that prohibit StorageGRID from being attached to ONTAP local tiers.

Errors might include the following examples:

- Unable to add cloud tier. Cannot verify the certificate provided by the object store server. The certificates might not be installed on the cluster. Do you want to add the certificate now?
- Cannot verify the certificate provided by the object store server.

To avoid these errors and successfully attach StorageGRID 11.2 and earlier as a cloud tier, you must replace the certificates in the grid with certificates that use the correct FQDN.

Although self-signed certificates can be used, using signed certificates from a third-party certificate authority is the recommended best practice.

Installation

To install CA certificates in ONTAP, complete the following steps:

1. Retrieve the CA certificates.
2. Install the certificates into ONTAP.

Retrieve CA Certificates

Retrieve the Root CA certificate and, if they exist, any intermediate CA certificates in Base-64 encoded format (sometimes also called PEM format) from the Certification Authority who created the certificate.

If you followed the procedure for StorageGRID SSL Certificate Configuration these are the certificates in the chain.pem file.

To retrieve the certificate for a StorageGRID endpoint, complete the following steps:

1. Open the StorageGRID Administration console.
2. Select Configuration > Load Balancer Endpoints.
3. Select your endpoint and click Edit Endpoint.
4. Copy the certificate PEM, including:

```
-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----
```
To retrieve the certificate when using a third-party load balancer, complete the following steps:

1. Run the following command:
   ```bash
   openssl s_client -connect <FQDN> -showcerts
   ```
   2. Copy the certificate, including:
   ```
   -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----
   ```

### Install Certificates to ONTAP

In ONTAP System Manager when adding a new Cloud Tier of type StorageGRID, you can paste the CA certificate. If there is an intermediate CA which issued the StorageGRID certificate, then this must be the intermediate CA certificate. If the StorageGRID certificate was issued directly by the Root CA, then you must use the Root CA certificate.

To install the Root certificates (and any intermediate certificates) to ONTAP, run the following command:

```bash
security certificate install -vserver <name> -type server-ca
```

### 4 Architecture

FabricPool works by associating a cloud tier (an external object store) with a local tier (storage aggregate) in ONTAP, creating a composite collection of discs: a FabricPool. Volumes inside the FabricPool can then take advantage of the tiering by keeping active (hot) data on performative SSDs (the local tier) and tiering inactivate (cold) data to the external object store (the cloud tier).

Although only a basic level of understanding is necessary to configure and use FabricPool, understanding how FabricPool determines block temperature, creates objects, and writes data is extremely useful when architecting storage solutions.

#### 4.1 Block Temperature

When a block is written to an SSD, it is assigned a temperature value indicating that it is hot. Over time, a background cooling scan cools blocks, making hot blocks warm and eventually turning blocks cold if they have not been read. Assuming no activity, a block becomes cold based on the time set by the tiering-minimum-cooling-days setting.

**Note:** The All volume tiering policy is an exception to this rule. Blocks in volumes using the All tiering policy are immediately identified as cold and marked for tiering.

#### 4.2 Object Creation

FabricPool works at the WAFL block level, cooling blocks, concatenating them into objects, and writing those objects to a cloud tier. Each FabricPool object is 4MB and composed of 1,024 4KB blocks. The object size is fixed at 4MB based on performance recommendations from leading cloud providers and cannot be changed. If cold blocks are read and made hot, only the requested blocks in the 4MB object are fetched. Neither the entire object nor the entire file is written back. Only the necessary blocks are written.

**Note:** If ONTAP detects an opportunity for sequential readahead, it requests blocks from the cloud tier before they are read in order to improve performance.

#### 4.3 Data Movement

After a block has been identified as cold, it is marked for tiering. During this time, a background tiering scan looks for cold blocks. When enough 4KB blocks from the same volume have been collected, they are concatenated into a 4MB object and moved to the cloud tier based on the volume tiering policy.
**Tiering Fullness Threshold**

By default, tiering to the cloud tier only happens if the local tier is >50% full. There is little reason to tier cold data to a cloud tier if the local tier is being underutilized.

In ONTAP 9.5, the 50% tiering fullness threshold is adjustable. Setting the threshold to a lower number reduces the amount of data required to be stored on the local tier before tiering takes place. This may be useful for large local tiers that contain little hot/active data.

Setting the threshold to a higher number increases the amount of data required to be stored on the local tier before tiering takes place. This may be useful for solutions designed to tier only when local tiers are near maximum capacity.

**Note:** The All volume tiering policy ignores the tiering fullness threshold. Blocks in volumes using the All tiering policy will be tiered irrespective of the tiering fullness threshold.

To change the tiering fullness threshold, run the following command:

```
storage aggregate object-store modify -aggregate <name> -tiering-fullness-threshold <#> (0%-99%)
```

**Note:** Advanced privilege level is required.

**Write-Back Prevention**

If the local tier is at >90% capacity, cold data is read directly from the cloud tier without being written back to the local tier. By preventing cold data write-backs on heavily utilized local tiers, FabricPool preserves the local tier for active data.

**SnapMirror Behavior**

Movement of data from the cloud tier to the local tier can take place any time a block is read.

**Table 1) SnapMirror behavior.**

<table>
<thead>
<tr>
<th>Source Volume Tiering Policy</th>
<th>Destination Volume Tiering Policy</th>
<th>Write Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto</td>
<td>Auto</td>
<td>Local &gt; Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cloud &gt; Cloud</td>
</tr>
<tr>
<td>Auto</td>
<td>Snapshot-Only</td>
<td>Local</td>
</tr>
<tr>
<td>Auto</td>
<td>All</td>
<td>Cloud</td>
</tr>
<tr>
<td>Auto</td>
<td>None</td>
<td>Local</td>
</tr>
<tr>
<td>Snapshot-Only</td>
<td>Auto</td>
<td>Local &gt; Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cloud &gt; Cloud</td>
</tr>
<tr>
<td>Snapshot-Only</td>
<td>Snapshot-Only</td>
<td>Local &gt; Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cloud &gt; Cloud</td>
</tr>
<tr>
<td>Snapshot-Only</td>
<td>All</td>
<td>Cloud</td>
</tr>
<tr>
<td>Snapshot-Only</td>
<td>None</td>
<td>Local</td>
</tr>
<tr>
<td>All</td>
<td>Auto</td>
<td>Local</td>
</tr>
<tr>
<td>All</td>
<td>Snapshot-Only</td>
<td>Local</td>
</tr>
<tr>
<td>All *</td>
<td>All *</td>
<td>Cloud*</td>
</tr>
</tbody>
</table>
**Volume Move**

Volume move (vol move) is the way that ONTAP moves a volume nondisruptively from one local tier (source) to another (destination). Volume moves can be performed for a variety of reasons, although the most common reasons are hardware lifecycle management, cluster expansion, and load balancing.

It is important to understand how volume move works with FabricPool because the changes that take place at both the local tier, the attached cloud tier, and the volume (volume tiering policies) can have a major impact on functionality.

**Destination Local Tier**

If a volume move’s destination local tier does not have an attached cloud tier, data on the source volume that is stored on the cloud tier is written to the local tier on the destination local tier.

Starting in ONTAP 9.6, if a volume move’s destination local tier uses the same bucket as the source local tier, data on the source volume that is stored in the bucket does not move back to the local tier. This optimized volume move results in significant network efficiencies.

**Note:** Some configurations are incompatible with optimized volume moves:

- Changing tiering policy during volume move
- Source and destination environment use different encryption settings
- FlexClone volumes
- FlexClone parent volumes
- MetroCluster
- Unsynced FabricPool Mirror buckets

If a volume move’s destination local tier has an attached cloud tier, data on the source volume that is stored on the cloud tier is first written to the local tier on the destination local tier. It is then written to the cloud tier on the destination local tier if this approach is appropriate for the volume’s tiering policy. Moving data to the local tier first improves the performance of the volume move and reduces cutover time.

If a volume tiering policy is not specified when performing a volume move, the destination volume uses the tiering policy of the source volume. If a different tiering policy is specified when performing the volume move, the destination volume is created with the specified tiering policy.

**Note:** When in an SVM-DR relationship, source and destination volumes must use the same tiering policy.
Minimum Cooling Days

Moving a volume to another local tier resets the inactivity period of blocks on the local tier. For example, a volume using the Auto volume tiering policy with data on the local tier that has been inactive for 20 days has data inactivity reset to 0 days after a volume move.

Auto

If `-tiering-policy auto` is specified during the volume move, data movement is variable, but all data moves to the destination local tier first.

If the source volume uses the Auto, None, or Snapshot-Only policy, blocks are moved to the same tier that they existed on prior to the move. If the source volume uses the All policy, all data is moved to the local tier.

```
vol move start -vserver <name> -volume <name> -destination-aggregate <name> -tiering-policy auto
```

Snapshot-Only

If `-tiering-policy snapshot-only` is specified during the volume move, data movement is variable, but data moves to the destination local first.

If both source and destination volumes use the Snapshot-Only policy, and the Snapshot block is being read from the source cloud tier, then FabricPool knows the Snapshot blocks are cold and moves the cold blocks to the destination cloud tier.

```
vol move start -vserver <name> -volume <name> -destination-aggregate <name> -tiering-policy snapshot-only
```

All

If `-tiering-policy all` is specified during the volume move, data is immediately identified as cold and written to the destination cloud tier. There is no need to wait 48 hours for blocks in the volume to become cold. Metadata is always stored on the local tier.

```
vol move start -vserver <name> -volume <name> -destination-aggregate <name> -tiering-policy all
```

None

If `-tiering-policy none` is specified during the volume move, data is written to the destination local tier.

```
vol move start -vserver <name> -volume <name> -destination-aggregate <name> -tiering-policy none
```
ONTAP System Manager
To perform a volume, move with ONTAP System Manager, complete the following steps:

1. Click STORAGE.
2. Click Volumes
3. Select the volume you want to move.
4. Click More.
5. Click Move.
6. Select a destination local tier.
7. Select a tiering policy.
8. Click Move.

Figure 8) Changing the volume tiering policy during a volume move.
ONTAP CLI

To perform a volume move using the ONTAP CLI, run the following command:

```
vol move start -vserver <name> -volume <name> -destination-aggregate <name> -tiering-policy <policy>
```

**FlexClone Volumes**

FlexClone volumes are copies of a parent FlexVol volume. Newly created FlexClone volumes inherit the volume tiering policy of the parent FlexVol volume. After a FlexVol volume has been created, the volume tiering policy can be changed.

FlexClone volumes that copy data protection destination volumes using the All tiering policy do not inherit the volume tiering policy of their parent. Instead, they are created using the Snapshot-Only policy.

If a FlexClone volume is split (volume clone split) from its parent volume, the copy operation writes the FlexClone volume’s blocks to the local tier.

**FlexGroup Volumes**

A FlexGroup volume is a single namespace that is made up of multiple constituent member volumes but is managed as a single volume. Individual files in a FlexGroup volume are allocated to individual member volumes and are not striped across volumes or nodes.

FlexGroup volumes are not constrained by the 100TB and two-billion file limitations of FlexVol volumes. Instead, FlexGroup volumes are only limited by the physical maximums of the underlying hardware and have been tested to 20PB and 400 billion files. Architectural maximums could be higher.

Volume tiering policies are set at the FlexGroup volume level—they cannot be set on the various constituent/member volumes that compose the FlexGroup volume.

When provisioning FlexGroup volumes on FabricPool local tiers, automatic processes require that the FlexGroup volume uses FabricPool local tier on every cluster node. This is a recommended best practice but not a requirement when manually provisioning FlexGroup volumes.

### 4.4 Object Storage

Object storage is a storage architecture that manages data as objects, as opposed to other storage architectures such as file or block storage. Objects are kept inside a single container (such as a bucket) and are not nested as files inside a directory inside other directories.

Although object storage is generally less performative than file or block storage, it is significantly more scalable. ONTAP currently has a maximum volume size of 100TB and a maximum local tier size of 800TB. Object stores have no such limits, and buckets with petabytes of data in them are not uncommon.

**FabricPool Cloud Tiers**

FabricPool currently supports object stores from multiple providers (Alibaba, Amazon, Google, IBM, Microsoft, NetApp, and so on) as cloud tiers.

More than one type of cloud tier can be used in a cluster. Usually one cloud tier is attached to each local tier but starting in ONTAP 9.7, FabricPool Mirror allows the attachment of two cloud tiers to a single local tier.
Object Deletion and Defragmentation

FabricPool does not delete blocks from attached object stores. Instead, FabricPool deletes entire objects after a certain percentage of the blocks in the object are no longer referenced by ONTAP.

For example, there are 1,024 4KB blocks in a 4MB object tiered to Amazon S3. Defragmentation and deletion do not occur until less than 205 4KB blocks (20% of 1,024) are being referenced by ONTAP. When enough (1,024) blocks have zero references, their original 4MB objects are deleted, and a new object is created.

This percentage, the unreclaimed space threshold, can be customized, but is set to different default levels for different object stores. The default settings are as follows:

- 12% Google Cloud Storage
- 14% IBM Cloud Object Storage
- 15% Alibaba Cloud Object Storage Service
- 15% Microsoft Azure Blob Storage
- 20% Amazon S3
- 40% StorageGRID

Unreclaimed Space Threshold

Object defragmentation reduces the amount of physical capacity used by the cloud tier at the expense of additional object store resources (reads and writes).

Reducing the Threshold

To avoid additional expenses, consider reducing the unreclaimed space thresholds when using object store pricing schemes that reduce the cost of storage but increase the cost of reads. Examples include Amazon’s Standard-IA and Azure Blob Storage’s cool.

For example, tiering a volume of 10-year-old projects that has been saved for legal reasons might be less expensive when using a pricing scheme such as Standard-IA or cool than it would be when using standard pricing schemes. Although reads are more expensive for such a volume, including reads required by object defragmentation, they are unlikely to occur frequently here.

Increasing the Threshold

Alternatively, consider increasing unreclaimed space thresholds if object fragmentation is resulting in significantly more object store capacity being used than necessary for the data being referenced by ONTAP. For example, using an unreclaimed space threshold of 20%, in a worst-case scenario where all objects are equally fragmented to the maximum allowable extent, it is possible for 80% of total capacity in the cloud tier to be unreferenced by ONTAP.

- 2TB referenced by ONTAP + 8TB unreferenced by ONTAP = 10TB total capacity used by the cloud tier.

In situations such as these, it might be advantageous to increase the unreclaimed space threshold—or increasing volume minimum cooling days—to reduce capacity being used by unreferenced blocks.

To change the default unreclaimed space threshold, run the following command:

```
storage aggregate object-store modify -aggregate <name> -object-store-name <name> -unreclaimed-space-threshold <%> (0%-99%)
```

(Advanced privilege level required.)

**Note:** Prior to ONTAP 9.4, object deletion takes place at an unreclaimed space threshold of 0%.
ONTAP Storage Efficiencies

Storage efficiencies such as compression, deduplication, and compaction are preserved when moving data to the cloud tier, reducing required object storage capacity and transport costs.

Aggregate inline deduplication is supported on the local tier, but associated storage efficiencies are not carried over to objects stored on the cloud tier.

When using the All volume tiering policy, storage efficiencies associated with background deduplication processes may be reduced as data will likely be tiered before the additional storage efficiencies can be applied.

Note: Third-party deduplication has not been qualified by NetApp.

5 Configuration

After the FabricPool basic requirements have been met, attaching a cloud tier to a local tier in ONTAP requires the following four steps:

1. Create a bucket/container on the object store.
2. Add a cloud tier using the bucket to ONTAP.
3. Attach the cloud tier to a local tier.
4. Set volume tiering policies.

5.1 Create a Bucket/Container

Buckets are object store containers that hold data. You must provide the name and location of the bucket in which data is stored before it can be added to a local tier as a cloud tier.

Buckets cannot be created using ONTAP System Manager, Active IQ (formerly OnCommand Unified Manager), or ONTAP.

Although FabricPool supports the attachment of two buckets (cloud tiers) per local tier using FabricPool Mirror, attaching a single cloud tier is more common.

A single cloud tier can be attached to a single local tier, and a single cloud tier can be attached to multiple local tiers. Attaching a single cloud tier to multiple local tiers in a cluster is the general best practice. NetApp does not recommend attaching a single cloud tier to local tiers in multiple clusters.

Note: Consider how cloud tier-to-local tier relationships might affect performance when planning storage architectures. Many public object store providers set a maximum number of supported IOPS at the bucket/container level. Environments that require maximum performance from public object stores should use multiple buckets to reduce the possibility that object-store IOPS limitations affect performance across multiple local tiers tiering to the same cloud tier.

Attaching a cloud tier to all FabricPool local tiers is the general best practice and provides significant benefits to environments that value manageability over public object store cloud tier performance.
Figure 9) Possible cloud tier-to-local tier relationships in ONTAP 9.7.

StorageGRID

To create a bucket in StorageGRID, complete the following steps using the StorageGRID Tenant Manager:

1. Open the Admin Node in a web browser (for example, https://admin.company.com/?accountId=###).
2. Log in with your tenant account ID, user name, and password.
3. Select S3.
4. Select Buckets.
5. Click Create Bucket.
6. Provide a DNS compliant name.
7. Click Save.

**Note:** Prior to StorageGRID 11.1, creating a bucket required using a third-party S3 client such as an S3 browser.

**Note:** ONTAP and StorageGRID system clocks must not be out of sync by more than a few minutes. Significant clock skew prevents the StorageGRID bucket from being attached to the local tier.
Other Object Store Providers

Instructions for creating buckets on other object store providers can be found on their respective sites:

- Alibaba Cloud Object Storage Service
- Amazon S3
- Google Cloud Storage
- IBM Cloud Object Storage
- Microsoft Azure Blob Storage

Other Object Store Provider Settings

FabricPool does not support ILM policies applied to object store buckets.

ILM typically includes various movement and deletion policies based on geography, storage class, retention, and other categories that would be disruptive to FabricPool cloud tier data. FabricPool has no knowledge of ILM policies or configurations set on external object stores, and misconfiguration of ILM policies can result in data loss.

Note: ONTAP and private cloud system clocks must not be out of sync by more than a few minutes. Significant clock skew will prevent the Cleversafe bucket from being attached to the local tier.

5.2 Add a Cloud Tier to ONTAP

Before a cloud tier can be attached to a local tier, it must be added to and identified by ONTAP. This task can be completed using either ONTAP System Manager or the ONTAP CLI.

You need the following information:

- Server name (FQDN) (for example, s3.amazonaws.com)
- Access key ID
- Secret key
- Container name (bucket name)

ONTAP System Manager

To add a cloud tier using ONTAP System Manager, complete the following steps:

1. Launch ONTAP System Manager.
2. Click STORAGE.
3. Click Tiers.
4. Click Add Cloud Tier.
5. Select an object store provider.
6. Complete the text fields as required for your object store provider.

   Note: Enter the object store’s bucket/container name in the Container Name field.

7. (Optional; cloud tiers can be attached to local tiers later if desired.) Add the cloud tier to local tiers as a primary cloud or as a FabricPool Mirror.

   Note: Attaching a cloud tier to a local tier is a permanent action. A cloud tier cannot be unattached from a local tier after being attached. (Using FabricPool Mirror, a different cloud tier can be attached.)

8. Click Save.
ONTAP CLI

To add a cloud tier using the ONTAP CLI, run the following commands:

```
object-store config create
-object-store-name <name>
-provider-type <AliCloud/AWS/Azure_Cloud/CAP/GoogleCloud/IBM_COS/S3_Compatible/SGWS>
-port <443/8082> (public clouds/SGWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

S3 Compatible Providers

Customers that want to use object stores that are not officially supported as a cloud tier can do so using –`provider-type S3_Compatible`. Customers will need to test and confirm that the object store meets their requirements.

NetApp does not support nor will be liable for any issues arising from any third-party Object Store Service, specifically where it does not have agreed support arrangements with the third party with whom the product originated. It is acknowledged and agreed that NetApp shall not be liable for any associated damage or otherwise be required to provide support on that 3rd party product.
Certificate Authority Certificate Validation

CA certificates associated with private cloud object stores, such as StorageGRID and some IBM Cloud Object Storage environments, should be installed on ONTAP before attaching them to local tiers. Using CA certificates creates a trusted relationship between ONTAP and the object store and helps to secure access to management interfaces, gateway nodes, and storage.

Failure to install a CA certificate results in an error unless certificate validation is turned off. Turning off certificate validation is not recommended, but it is possible starting in ONTAP 9.4.

ONTAP System Manager

CA certificate validation can be turned off when adding a StorageGRID cloud tier using ONTAP System Manager. To do so, complete the following steps:

1. Launch ONTAP System Manager.
2. Click STORAGE.
3. Click Tiers.
4. Click Add Cloud Tier.
5. Select an object store provider.
6. Complete the text fields as required for your object store provider.
7. Click the Object Store Certificate button to turn it off.

   **Note:** Turning off certificate validation is not recommended.
8. Click Save.

Figure 11) Add object store certificate.
ONTAP CLI

CA certificate validation can be turned off when adding a private cloud tier using the ONTAP CLI. To do so, run the following commands:

```bash
object-store config create
  -object-store-name <name>
  -provider-type <AWS/Azure_Cloud/IBM_COS/SGWS>
  -port <443/8082> (AWS&Azure_Cloud&IBM_COS/SGWS)
  -server <name>
  -container-name <bucket-name>
  -access-key <string>
  -secret-password <string>
  -ssl-enabled true
  -ipspace default
  -is-certificate-validation-enabled false
```

5.3 Attach a Cloud Tier to a Local Tier

After an object store has been added to and identified by ONTAP as a cloud tier, it can be attached to a local tier to create a FabricPool. This task can be completed using either ONTAP System Manager or the ONTAP CLI.

**Note:** Attaching a cloud tier to a local tier is a permanent action. A cloud tier cannot be unattached from a local tier after being attached. (Using FabricPool Mirror, a different cloud tier can be attached.)

Thin Provisioning

FabricPool cannot attach a cloud tier to a local tier that contains volumes using a space guarantee other than none (for example, volume). For additional information, refer to FabricPool’s requirements.

FlexGroup Volumes

All local tiers used by a FlexGroup volume must be FabricPool local tiers.

When provisioning FlexGroup volumes on FabricPool local tiers, automatic processes require that the FlexGroup volume uses FabricPool local tiers on every cluster node. This is a recommended best practice but is not a requirement when manually provisioning FlexGroup volumes.

**Note:** Consider how cloud tier-to-local tier relationships might affect performance when planning storage architectures. Many public object store providers set a maximum number of supported IOPS at the bucket/container level. Environments that require maximum performance from public object stores should use multiple buckets to reduce the possibility that object-store IOPS limitations affect performance across multiple local tiers tiering to the same cloud tier.

Attaching a cloud tier to all FabricPool local tiers is the general best practice and provides significant benefits to environments that value manageability over public object store cloud tier performance.
ONTAP System Manager

To attach a cloud tier to a local tier using ONTAP System Manager, complete the following steps:

1. Launch ONTAP System Manager.
2. Click STORAGE.
3. Click the name of a local tier.
4. Click More.
5. Click Attach Cloud Tiers.
6. Select the primary cloud tier to attach.
7. Select volumes to set tiering policies.
8. Click Save.

   **Note:** Attaching a cloud tier to a local tier is a permanent action. A cloud tier cannot be unattached from a local tier after being attached. (Using FabricPool Mirror, a different cloud tier can be attached.)

![Attach Cloud Tiers](image)

Figure 12) Attach cloud tier.
ONTAP CLI

To attach a cloud tier to a local tier (storage aggregate) using the ONTAP CLI, run the following commands:

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

**Example:**

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name aws_fabricpool_bucket
```

**Note:** Attaching a cloud tier to a local tier is a permanent action. A cloud tier cannot be unattached from a local tier after being attached. (Using FabricPool Mirror, a different cloud tier can be attached.)

**FlexGroup Volumes**

To list the local tiers used by a FlexGroup volume, and attach a cloud tier to those local tiers using the ONTAP CLI, run the following commands:

```
volume show -volume <name> -fields aggr-list
```

Then:

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
-allow-flexgroup true
```

### 5.4 Set Volume Tiering Policies

By default, volumes use the None volume tiering policy. After volume creation, the volume tiering policy can be changed using ONTAP System Manager or the ONTAP CLI.

FabricPool provides four volume tiering policies, as described in the following sections.

**Note:** When used by FlexGroup volumes, the volume tiering policy is set at the FlexGroup volume level. Volume tiering policies cannot be set on the various constituent/member volumes that compose the FlexGroup volume.

- **Auto:**
  - All cold blocks in the volume are moved to the cloud tier. Assuming the local tier is >50% utilized, it takes approximately 31 days for inactive blocks to become cold. The Auto cooling period is adjustable between 2 days and 63 days using `tiering-minimum-cooling-days`.
  - When cold blocks in a volume with a tiering policy set to Auto are read randomly, they are made hot and written to the local tier.
  - When cold blocks in a volume with a tiering policy set to Auto are read sequentially, they stay cold and remain on the cloud tier. They are not written to the local tier.

- **Snapshot-Only:**
  - Cold Snapshot blocks in the volume that are not shared with the active file system are moved to the cloud tier. Assuming the local tier is >50% utilized, it takes approximately two days for inactive Snapshot blocks to become cold. The Snapshot-Only cooling period is adjustable from 2 to 63 days using `tiering-minimum-cooling-days`.
  - When cold blocks in a volume with a tiering policy set to Snapshot-Only are read, they are made hot and written to the local tier.
• **All:**
  - All data blocks (not including metadata) placed in the volume are immediately marked as cold and moved to the cloud tier as soon as possible. There is no need to wait 48 hours for new blocks in a volume using the All tiering policy to become cold.
  - Blocks located in the volume prior to the All policy being set require 48 hours to become cold.
  - When cold blocks in a volume with a tiering policy set to All are read, they remain cold and stay on the cloud tier. They are not written to the local tier.
  - Prior to ONTAP 9.6, the Backup volume tiering policy functioned the same as the All policy with the exception that the Backup policy can only be set on data protection volumes (destination targets).

**Note:** Object storage is not transactional like file or block storage. Making changes to files being stored as objects in volumes using the All tiering policy can result in the creation of new objects, fragmentation of existing objects, and the addition of storage inefficiencies.

Because the All tiering policy tiers data as soon as possible, storage efficiencies that rely on background processes, like deduplication, might not have enough time to be applied. Inline storage efficiencies like compression and compaction are still applied.

Consider the impact of SnapMirror transfers before assigning the All tiering policy to source volumes in data protection relationships. Because data is tiered immediately, SnapMirror will read data from the cloud tier rather than the local tier. This will result in slower SnapMirror operations—possibly slowing other SnapMirror operations later in queue—even if they are using different tiering policies.

• **None (default):**
  - Volumes set to use none as their tiering policy do not tier cold data to the cloud tier.
  - Setting the tiering policy to none prevents new tiering. Volume data that has previously been moved to the cloud tier remains in the cloud tier until it becomes hot and is automatically moved back to the local tier.
  - When cold blocks in a volume with a tiering policy set to none are read, they are made hot and written to the local tier.

**ONTAP System Manager**

To change a volume’s tiering policy by using ONTAP System Manager, complete the following steps:

1. Launch ONTAP System Manager.
2. Click STORAGE.
3. Click Volumes.
4. Select a volume.
5. Click Edit.
6. Select the tiering policy you want to apply to the volume.
7. Click Save.
ONTAP CLI

To change a volume’s tiering policy using the ONTAP CLI, run the following command:

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-policy <auto|snapshot-only|all|none>
```

**Note:** The default volume tiering policy is None.

### 5.5 Set Volume Tiering Minimum Cooling Days

The tiering-minimum-cooling-days setting determines how many days must pass before inactive data in a volume using the Auto or Snapshot-Only policy is considered cold and eligible for tiering.

**Auto**

The default tiering-minimum-cooling-days setting for the Auto tiering policy is 31 days.

Because reads keep block temperatures hot, increasing this value might reduce the amount of data that is eligible to be tiered and increase the amount of data kept on the local tier.

If you would like to reduce this value from the default 31-days, be aware that data should no longer be active before being marked as cold. For example, if a multi-day workload is expected to perform a significant number of writes on day seven, the volume’s tiering-minimum-cooling-days setting should be set no lower than eight days.

Object storage is not transactional like file or block storage. Making changes to files being stored as objects in volumes with overly aggressive minimum cooling days can result in the creation of new objects, fragmentation of existing objects, and the addition of storage inefficiencies.

**Snapshot-Only**

The default tiering-minimum-cooling-days setting for the Snapshot-Only tiering policy is two days. A two-day minimum provides additional time for background processes to provide maximum storage efficiency and prevents daily data-protection processes from needing to read data from the cloud tier.

ONTAP CLI

To change a volume’s tiering minimum cooling days setting using the ONTAP CLI, run the following command:

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum-cooling-days <2-63>
```

(Advanced privilege level required.)

**Note:** Changing the tiering policy between Auto and Snapshot-Only (or vice versa) resets the inactivity period of blocks on the local tier. For example, a volume using the Auto volume tiering policy with data on the local tier that has been inactive for 20 days, will have the local tier data inactivity reset to 0 days if the tiering policy is set to Snapshot-Only.
5.6 FabricPool Mirror

More than one type of cloud tier can be used in a cluster, but usually a single cloud tier is attached to a single local tier. Starting in ONTAP 9.7, FabricPool Mirror allows the attachment of two cloud tiers to a single local tier, creating additional options for data availability and movement.

When using FabricPool Mirror, data is mirrored across two buckets. During bucket synchronization, data will need to be read from the pre-existing primary bucket and written to the secondary bucket. This synchronization is necessary to achieve a mirrored state between the two buckets.

When both buckets are in a mirrored state, newly tiered data is synchronously tiered to both buckets. Because data is being tiered to two buckets synchronously, the effective throughput will be half of standard single-bucket tiering. For example, if PUTs to a single bucket took place at 600MBps, PUTs to mirrored buckets in a FabricPool Mirror deployment would take place at 300MBps.

Under normal circumstances, all GET operations take place from the primary bucket. Only if connectivity is interrupted to the primary bucket will GET operations take place from the secondary bucket.

If connectivity is lost to either bucket, tiering will temporarily be suspended until connectivity is established.

**Note:** Although essential for FabricPool with NetApp MetroCluster™, FabricPool Mirror is a stand-alone feature that does not require MetroCluster to use.

Figure 13) FabricPool containing one local tier and two cloud tiers.

When adding FabricPool Mirror to an existing FabricPool, data previously tiered to the original cloud tier read from the primary bucket is written to the newly attached secondary bucket.

**Note:** Public cloud charges for reads and writes apply to both buckets as normal.
Licensed Capacity

During synchronization, the FabricPool capacity license will apply equally to both cloud tiers.

For example, a cluster with a 100TB license and 75TB of data in Bucket A will be able to mirror 75TB of data to Bucket B. A total of 150TB has been tiered even though the FabricPool license is only for 100TB of capacity.

After both tiers are mirrored, licensed capacity will apply as normal and tiering to the cloud tier will stop if the amount of data (used capacity) tiered to both cloud tiers is greater than the licensed capacity.

For example, a cluster with a 100TB FabricPool license and 75TB of tiered data in Bucket A, and 75TB of tiered data mirrored to Bucket B, will be using 150TB of capacity. The cluster will need to increase the FabricPool license to >150TB to tier additional data.

Figure 14) 75TB can be mirrored to another bucket but additional tiering will stop until the license is increased. The used capacity, 150TB, is greater than the 100TB licensed capacity.

Newly tiered data is synchronously tiered to both cloud tiers provided it is supported by the licensed capacity.

For example, a cluster with a 200TB license and 75TB of tiered data in Bucket A, and 75TB of tiered data mirrored to Bucket B, will be using 150TB of capacity. FabricPool will continue to tier data to both cloud tiers until both buckets contain 100TB of tiered data.

Figure 15) A 200TB FabricPool license will support mirroring 75TB to two buckets. The licensed capacity, 200TB, is greater than the 150TB used capacity.
Multicloud Solutions

Object stores are generally designed to provide 99.999999999% (11 9s) durability and 99.99% (4 9s) availability. Given 525,600 minutes in a year, 99.99% availability allows for one minute of unavailability per year.

For customers who need better availability, FabricPool Mirror can be used to tier data to multiple cloud vendors for an additional level of resiliency as the likelihood that multiple cloud providers experiences outages at the same time is extremely rare. Using a single cloud vendor, but different regions or availability zones (for example, Google’s europe-west3-a and europe-west6-a) as an alternative to using multiple providers.

During bucket synchronization, data will need to be read from the pre-existing primary bucket and written to the secondary bucket. Reads from public clouds will be subject to egress fees.

**Note:** When applicable, after a synchronous mirror has been established between two cloud tiers, the total amount of data tiered to both cloud tiers is applied to the FabricPool license.

Enhanced Data Mobility

FabricPool has always allowed for data mobility, but prior to ONTAP 9.7, a volume move was required to nondisruptively move from one FabricPool to another. Although a simple process, volume moves require that the destination local tier has enough capacity to hold the volume being moved.

FabricPool Mirror can be used to change the cloud tier attached to a local tier without having to perform a volume move by:

1. Adding a secondary cloud tier to the local tier.
2. Waiting for a synchronous mirror to be established between the primary and secondary cloud tiers.
3. Swapping cloud tiers so the primary and secondary cloud tier relationships change. The secondary cloud tier becomes the new primary cloud tier and the original primary cloud tier becomes the new secondary cloud tier.
4. Deleting the FabricPool Mirror.

ONTAP System Manager

**Attach**

To attach an additional cloud tier, a FabricPool Mirror, to a local tier using ONTAP System Manager, complete the following steps:

1. Launch ONTAP System Manager.
2. Click Attach FabricPool Mirror.
3. Select a cloud tier to use as the secondary cloud tier.
4. Click Save.

**Swap**

To swap cloud tiers so the primary and secondary cloud tier relationships change in a FabricPool Mirror using ONTAP System Manager, complete the following steps:

1. Launch ONTAP System Manager.
2. Click Storage.
3. Click Tiers.
4. Click the name of the local tier you wish to remove the FabricPool Mirror from.
5. Click More.
6. Click Swap Cloud Tiers.

![Swap Primary Cloud Tier with FabricPool Mirror](image)

7. Click Swap.

**Delete**

To remove the FabricPool Mirror using ONTAP System Manager, complete the following steps:

1. Launch ONTAP System Manager.
2. Click Storage.
3. Click Tiers.
4. Click the name of the local tier you wish to remove the FabricPool Mirror from.
5. Click More.
6. Click Delete FabricPool Mirror.
7. Click Delete.

**ONTAP CLI**

**Attach**

To attach an additional cloud tier, a FabricPool Mirror, to a local tier (storage aggregate) using the ONTAP CLI, run the following commands:

```
storage aggregate object-store mirror -aggregate <aggregate name> -name <object-store-name-2>
```

**Swap**

To swap cloud tiers so the primary and secondary cloud tier relationships change in a FabricPool Mirror using the ONTAP CLI, run the following commands:

```
storage aggregate object-store modify -aggregate <aggregate name> -name <object-store-name-2> -mirror-type primary
```

**Delete**

To remove the FabricPool Mirror, using the ONTAP CLI, run the following commands:
5.7 MetroCluster

MetroCluster provides continuous data availability across geographically separated data centers for mission-critical applications. MetroCluster continuous availability and disaster recovery software runs on ONTAP data management software. Both FC and Ethernet (IP) MetroCluster configurations are used by thousands of enterprises worldwide for high availability, zero data loss, and nondisruptive operations both within and beyond the data center.


When using FabricPool Mirror, data is mirrored across two buckets so Cluster A’s local tiers can be connected to cloud tier A (primary) and cloud tier B (mirror) and Cluster B’s local tiers can be connected to cloud tier B (primary) and cloud tier A (mirror), as shown in Figure 16.

Figure 16) MetroCluster + FabricPool.

Note: In order to successfully create a FabricPool aggregate in MetroCluster, both buckets must be accessible from both clusters.
Licensed Capacity

FabricPool licensed capacity applies equally to both buckets in a MetroCluster configuration.

Unmirrored Aggregates/Local Tiers

MetroCluster expects all local tiers, both traditional aggregates, and those using FabricPool, to be mirrored. Unmirrored aggregates in MetroCluster environments do not need to use FabricPool Mirror, but they generate messages warning that the aggregate is not mirrored, and when using FabricPool, that they are missing a FabricPool Mirror.

To view the MetroCluster error messages, run the following command:

```
metrocluster check show
```

5.8 Security

FabricPool maintains AES-256-GCM encryption on the local tier, on the cloud tier, and over the wire when moving data between the tiers.

Local Tier

FabricPool supports NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE), and NetApp Aggregate Encryption (NAE). Neither NSE, NVE, nor NAE are required to use FabricPool.

Over the Wire

Objects moving between local and cloud tiers are encrypted by using TLS 1.2 using AES-256-GCM. Other encryption modes, such as CCM, are not supported. To some extent, encryption affects connectivity (latency) because object stores must use CPU cycles to decrypt the data. Communicating with object stores without TLS encryption is supported but is not recommended.

Cloud Tier

All objects encrypted by NVE/NAE remain encrypted when moved to the cloud tier. Client-side encryption keys are owned by ONTAP.

All objects not encrypted using NVE/NAE are automatically encrypted server-side using AES-256-GCM encryption. No additional encryption is necessary. Server-side encryption keys are owned by the respective object store.

Note: FabricPool requires the use of the AES-256-GCM authenticated encryption. Other encryption modes, such as CCM, are not supported.

Disabling Cloud Tier Encryption

Starting in ONTAP 9.7, encrypting cold data at rest is no longer required. Using FabricPool without encrypting data at rest is not recommended but may be required by low performance S3 compatible object storage providers who cannot provide server-side encryption and low latency at the same time. NetApp highly recommends using client-side NVE or NVA encryption in these circumstances as encrypting data at rest remains the recommended best practice.

To disable cloud tier encryption, run the following command:

```
storage aggregate object-store config modify -serverside-encryption false
```

(Advanced privilege level is required.)
6 Interoperability

In general, ONTAP functionality is unchanged on FabricPool local tiers. Although ONTAP must create and transfer objects and blocks between local and cloud tiers, data protection, efficiency, and security are nearly identical to standard local tiers in ONTAP. The primary differentiators are performance and cost, with object stores being slower and less expensive.

The exceptions to normal interoperability listed in Table 2 and Table 3 are unique to FabricPool local tiers.

Table 2) NetApp interoperability.

<table>
<thead>
<tr>
<th>Focus</th>
<th>Supported</th>
<th>Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud tier</td>
<td>StorageGRID 10.3+</td>
<td>ONTAP local tiers</td>
</tr>
<tr>
<td>Data protection</td>
<td>• MetroCluster</td>
<td>• 7-Mode Data Transition Using SnapMirror</td>
</tr>
<tr>
<td></td>
<td>• MetroCluster SDS</td>
<td>• 7-Mode Transition Tool (7MTT)</td>
</tr>
<tr>
<td></td>
<td>• SnapMirror (XDP and DP)</td>
<td>• DP_Optimized license (DPO)</td>
</tr>
<tr>
<td></td>
<td>• SnapMirror Synchronous</td>
<td>• NetApp SyncMirror&lt;sup&gt;®&lt;/sup&gt; technology</td>
</tr>
<tr>
<td></td>
<td>• SnapVault (XDP and DP)</td>
<td>• Cascading SnapMirror relationships using the All (or Backup) tiering policy.</td>
</tr>
<tr>
<td></td>
<td>• SVM-DR</td>
<td>• SMTape</td>
</tr>
<tr>
<td></td>
<td>• StorageGRID replication and erasure coding</td>
<td>• NetApp SnapLock&lt;sup&gt;®&lt;/sup&gt; technology</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For best results, use replication with StorageGRID 11.2 or lower and erasure coding with StorageGRID 11.3+.</td>
<td>• StorageGRID ILM policies other than replication and erasure coding</td>
</tr>
<tr>
<td>Encryption</td>
<td>• NetApp Volume Encryption</td>
<td>• Object versioning</td>
</tr>
<tr>
<td></td>
<td>• NetApp Storage Encryption</td>
<td>• WORM</td>
</tr>
<tr>
<td></td>
<td>• Server-side encryption (AES-256)</td>
<td>• StorageGRID Compliance buckets</td>
</tr>
<tr>
<td></td>
<td>• TLS 1.2</td>
<td></td>
</tr>
<tr>
<td>Storage efficiency</td>
<td>• Inline deduplication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Inline compression</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Compaction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Aggregate inline deduplication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (local tier only)</td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td>–</td>
<td>NetApp FlexArray&lt;sup&gt;®&lt;/sup&gt; technology</td>
</tr>
<tr>
<td>virtualization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality of service (QoS)</td>
<td>QoS maximums (ceiling)</td>
<td>QoS minimums (floors)</td>
</tr>
<tr>
<td>Additional</td>
<td>–</td>
<td>Auto Balance Aggregate Flash Pools</td>
</tr>
<tr>
<td>features</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Focus

<table>
<thead>
<tr>
<th>Supported</th>
<th>Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud tier</td>
<td>Alibaba Archive, Amazon Glacier, Azure Archive, IBM Archive</td>
</tr>
<tr>
<td>Alibaba Cloud Object Storage Service (Standard, Infrequent Access)</td>
<td></td>
</tr>
<tr>
<td>Amazon S3 (Standard, Standard-IA, One Zone-IA, Intelligent-Tiering)</td>
<td></td>
</tr>
<tr>
<td>Amazon Commercial Cloud Services (C2S)</td>
<td></td>
</tr>
<tr>
<td>Google Cloud Storage (Multi-Regional, Regional, Nearline, Coldline, Archive)</td>
<td></td>
</tr>
<tr>
<td>IBM Cloud Object Storage (including Cleversafe and SoftLayer)</td>
<td></td>
</tr>
<tr>
<td>Microsoft Azure Blob Storage (Hot and Cool)</td>
<td></td>
</tr>
<tr>
<td>StorageGRID 10.3+</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data protection</th>
<th>ILM policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon’s 99.999999999% multi-region durability</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encryption</th>
<th>–</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server-side encryption (AES-256)</td>
<td></td>
</tr>
<tr>
<td>TLS 1.2</td>
<td></td>
</tr>
</tbody>
</table>

## 6.1 StorageGRID

### Performance

Unlike public clouds that might set a maximum number of supported IOPS at the bucket/container level, StorageGRID performance scales with the number of nodes in the system.

NetApp recommends provisioning enough StorageGRID nodes to meet or exceed capacity and performance requirements.

### Load Balancing

StorageGRID includes an optional load balancer called the API Gateway Node. Although the API Gateway Node is low cost and requires no configuration, it is not as robust as other load-balancer options.

Grids that act as cloud tiers for applications that need immediate access to data should consider using appliance-based load balancers, such as the SG1000.

For additional information refer to TR-4626: StorageGRID Load Balancer Options.

**Note:** With StorageGRID 11.3, High-availability (HA) groups can be used to provide highly available data connections for S3 client. HA groups can also be used to provide highly available connections to the Grid Manager and the Tenant Manager. High availability groups use virtual IP addresses (VIPs) to provide active-backup access to Gateway Node or Admin Node services.

### Storage Efficiency

ONTAP’s volume-level storage efficiencies such as compression, deduplication, and compaction are preserved when moving data to the cloud tier. NetApp recommends disabling stored object compression in StorageGRID.
Security

All data encrypted by ONTAP NVE/NAE remains encrypted when moved to the cloud tier. Client-side encryption keys are owned by ONTAP.

All objects not encrypted using ONTAP NVE/NAE are automatically encrypted by StorageGRID using AES-256-GCM encryption. No additional encryption is necessary. NetApp recommends disabling stored object encryption in StorageGRID.

Data Protection

StorageGRID uses two-copy replication as the default ILM rule for data protection. As of StorageGRID 11.2+, intrasite erasure coding using a 2+1 scheme is the recommended best practice for cost efficient data protection.

Erasure coding uses more CPU, but significantly less storage capacity, than replication. 4+1 and 6+1 schemes will use even less capacity than 2+1, but at the cost of lower throughput and less flexibility when adding storage nodes during grid expansion.

Note: Single copy replication is not recommended due to lowered system availability and data durability. Geographically dispersed erasure coding such as 4+2 or 6+3 over multiple physical sites is not recommended due to additional latencies. Geographically dispersed erasure coding such as 4+2 or 6+3 over multiple physical sites is not recommended due to additional latencies.

Information Lifecycle Management

FabricPool supports StorageGRID’s information lifecycle management (ILM) policies for data replication and erasure coding to protect cloud tier data from failure. However, FabricPool does not support advanced ILM rules such as filtering based on user metadata or tags.

ILM can include various movement and deletion policies based on geography, storage class, retention, and other categories that would be disruptive to FabricPool cloud tier data. FabricPool has no knowledge of ILM policies or configurations set on external object stores, and misconfiguration of ILM policies can result in data loss. For example, FabricPool cloud tier data must not be expired/deleted or moved out of the bucket to other locations (Archive, Glacier, and so on).

Virtualized Nodes

In addition to performance-optimized hardware appliances, StorageGRID nodes can be deployed as virtual machines (VMs) or Docker containers. Do not host virtualized nodes in ONTAP volumes that tier inactive data. Set the tiering policy on those volumes to None.

Failure to set the tiering policy to None can place the virtualized object store at risk as blocks associated with the VMs can be marked as cold and tiered into themselves, causing significant spikes in latency and reductions in throughput when read.
7 Performance

7.1 Sizing the Local Tier

When considering sizing, the local tier should be capable of the following tasks:

- Supporting hot data
- Supporting cold data until the tiering scan moves the data to the cloud tier
- Supporting cloud tier data that becomes hot and is written back to the local tier
- Supporting WAFL metadata associated with the attached cloud tier

For most environments, a 1 : 10 :: local tier : cloud tier ratio is extremely conservative while providing significant storage savings.

Note: Writes from the cloud tier to the local tier are disabled if local tier capacity is greater than 90%. If this occurs, blocks are read directly from the cloud tier.

7.2 Sizing the Cloud Tier

When considering sizing, the object store acting as the cloud tier should be capable of the following tasks:

- Supporting reads of existing cold data
- Supporting writes of new cold data
- Supporting object deletion and defragmentation

Inactive Data Reporting

First available in ONTAP 9.4, inactive data reporting (IDR) is an excellent tool for determining the amount of inactive (cold) data that can be tiered from a local tier.

IDR uses a 31-day cooling period to determine what data is considered inactive. The amount of cold data that is tiered is dependent on the tiering policies set on volumes. This amount might be different than the amount of cold data detected by IDR using a 31-day cooling period.

- IDR is enabled by default on all SSD local tiers in ONTAP 9.6.
- IDR is enabled by default on FabricPool local tiers in ONTAP 9.4 and ONTAP 9.5.
- IDR can be enabled on non-FabricPool local tiers using the ONTAP CLI. This includes HDD local tiers starting in ONTAP 9.6.
- IDR cannot be enabled for situations in which FabricPool cannot be enabled: for example, root local tiers, local tiers with space provisioning, Flash Pools, and so on.

Table 4) IDR behavior.

<table>
<thead>
<tr>
<th>ONTAP Version</th>
<th>IDR Enabled</th>
<th>Tiering Policy</th>
<th>Behavior</th>
<th>Window</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.4 – 9.7</td>
<td>Yes</td>
<td>None</td>
<td>Reports all cold data</td>
<td>31 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Snapshot-Only</td>
<td>Reports all cold data</td>
<td>31 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: Snapshot blocks would have already been tiered by using the default two-day setting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Auto</td>
<td>Does not report IDR</td>
<td>Inactive data has already tiered</td>
</tr>
</tbody>
</table>
### ONTAP System Manager

IDR is displayed on the local tiers overview in ONTAP System Manager.

**Figure 17**) IDR in ONTAP System Manager.

![ONTAP System Manager IDR](image)

### ONTAP CLI

To enable IDR on a non-FabricPool local tier, run the following command:

```
storage aggregate modify -aggregate <name> -is-inactive-data-reporting-enabled true
```

To display IDR by using the ONTAP CLI, run the following command:

```
storage aggregate show-space -fields performance-tier-inactive-user-data, performance-tier-inactive-user-data-percent
```

The `performance-tier-inactive-user-data-percent` field displays what percent of the volume’s total capacity is inactive, not the percent of the volume’s used capacity.

**Note:** Although IDR is enabled by default on all SSD local tiers (ONTAP 9.6+), if a client workload needs 100% of system resources, it will automatically turn off, resetting cooling days to zero. If this happens, IDR will not automatically turn back on.
To avoid automated process shutting off IDR in order to free up resources for other workloads, manually enable `-is-inactive-data-reporting-enabled` to `true`.

### 7.3 Connectivity

FabricPool read latency is a function of connectivity to the cloud tier. LIFs using 10Gbps ports provide adequate performance. NetApp recommends validating the latency and throughput of your specific network environment to determine the impact it has on FabricPool performance.

**Object Store Profiler**

Starting in ONTAP 9.4, an object store profiler is available through the CLI that lets you test latency and throughput performance of object stores before you attach them to FabricPool local tiers.

**Note:** The cloud tier must be added to ONTAP before it can be used with the object store profiler.

Start the object store profiler.

```
storage aggregate object-store profiler start -object-store-name <name> -node <name>
```

(Advanced privilege level required.)

View the results.

```
storage aggregate object-store profiler show
```

**Note:** Cloud tiers do not provide performance similar to that found on the local tier (typically GB per second).

Although cloud tiers can easily provide SATA-like performance, they can also tolerate latencies as high as 10 seconds and low throughputs for tiering solutions that do not need SATA-like performance.

When using FabricPool in low-performance environments, minimum performance requirements for client applications must continue to be met, and recovery time objectives (RTOs) should be adjusted accordingly.

**Network Connections**

Although direct connections provide better performance and lower data transfer charges, they are not required by FabricPool. Because performance can be significantly better when using direct connections, doing so using 10Gbps is the recommended best practice for FabricPool.

- Alibaba Cloud Object Storage Service (Express Connect)
- Amazon S3 (Direct Connect)
- Google Cloud Storage (Cloud Interconnect)
- IBM Cloud Object Storage (Direct Link)
- Microsoft Azure Blob Storage (ExpressRoute)

**StorageGRID**

Unlike public clouds that might set a maximum number of supported IOPS at the bucket/container level, StorageGRID performance scales with the number of nodes in a system. For acceptable performance targets, NetApp recommends using enough nodes to meet or exceed FabricPool connectivity requirements.
SnapMirror Concurrency

Because concurrent SnapMirror and SnapVault replication operations share the network link to the cloud tier, initialization and RTO are dependent on the available bandwidth and latency to the cloud tier. Performance degradation might occur if connectivity resources become saturated.

Proactive configuration of multiple LIFs can significantly decrease this type of network saturation.

**Note:** If you are using more than one IC LIF on a node with different routing, NetApp recommends placing them in different IPspaces. During configuration, FabricPool can select from multiple IPspaces, but it is unable to select specific IC LIFs within an IPspace.

Loss of Connectivity

If for any reason connectivity to the cloud is lost, the FabricPool local tier remains online, but applications receive an error message when attempting to get data from the cloud tier. Cold blocks that exist exclusively on the cloud tier remain unavailable until connectivity is reestablished.

**NAS Protocols**

NFS and SMB protocols generally retry every five seconds until a connection is reestablished.  

Error messages include the following:

- **SMB**
  
  STATUS_INTERNAL_ERROR

  Client applications might or might not retry upon receiving this error (this is client dependent). The client does not have to remount.

- **NFS**
  
  v3: EJUKEBOX  
  
  v4: EDELAY

  NFS client applications retry after five seconds. The NFS client hangs until connectivity is reestablished if it gets the same error after a retry.

**SAN Protocols**

FC and iSCSI protocols generally take longer before experiencing a timeout (60–120 seconds), but they do not retry to establish a connection in the same way NAS protocols do. If a SAN protocol times out, the application must be restarted.

Even a short disruption could be disastrous to production applications using SAN protocols because there is no way to guarantee connectivity to public clouds. To avoid this, NetApp recommends using private clouds, like StorageGRID, when tiering data that is accessed by SAN protocols.

- **SAN**
  
  UNRECOVERED READ ERROR/RECOMMEND REWRITE THE DATA

  If the host is connected to the ONTAP LUN and the LUN is configured in a RAID set on the host (for example, Volume Manager), the host RAID subsystem might be able to recover the data from parity, and the data is rewritten to a new location. If the host is unable to recover this data, then the application on the host might need to be restarted so that the read can be retried.
7.4 Capacity

Storage Tiers

NetApp’s recommended 1:10 local tier:cloud tier ratio is conservative. FabricPool continues to tier cold data to a cloud tier until the local tier reaches 98% capacity. For example, an 800TB local tier will reach 98% capacity at 784TB. Given a dataset using 5% metadata, 15.6PB could have been tiered to the cloud before reaching 784TB on the local tier.

Because of the difference in ingress and egress rates, it is possible run out of space on a small local tier when attempting to move more data than it has capacity to hold. Data is usually coming into the local tier at a faster rate than it can be converted into objects and tiered out.

For example, if a volume move takes place at 2GBps but tiering takes place at 500MBps, 50TB completes the volume move to the local tier in ~7 hours. However, ~28 hours are required for tiering to an object store. The local tier must have enough capacity to store the data before it is tiered. Local space utilization can be determined by using ONTAP System Manager or the ONTAP CLI.

ONTAP System Manager

In ONTAP System Manager, FabricPool space utilization is displayed on the local tiers overview. Details include local tier maximum capacity, used capacity, and external tier used capacity.

Figure 18) FabricPool space utilization information.

ONTAP CLI

To view FabricPool space utilization details using the ONTAP CLI, run the following command:

```
storage aggregate object-store show-space
```
Volumes

FlexVol volumes in a FabricPool local tier cannot exceed the 100TB maximum volume size for FlexVols regardless of what tier the data is located on. For example, a FlexVol with 1TB on the local tier and 99TB on the cloud tier has reached the 100TB maximum FlexVol size, even though only 1TB is stored on the local tier.

Unlike FlexVol volumes, FlexGroup volumes have virtually no capacity or file count constraints outside of the physical limits of hardware or the total volume limits of ONTAP.

If the local tier reaches 98% capacity, FabricPool stops tiering cold data to the cloud tier. If the local tier reaches 90% capacity, cold data is read directly from the cloud tier without being written back to the local tier.

FabricPool volume space utilization can be determined by using ONTAP System Manager or the ONTAP CLI.

ONTAP CLI

View FabricPool volume space utilization details using the ONTAP CLI.

```
volume show-footprint
```

Total, local tier (performance tier), and cloud tier (using the bucket name) footprints are displayed.

```
Vserver : svm_fabricpool
Volume : project_b

<table>
<thead>
<tr>
<th>Feature</th>
<th>Used</th>
<th>Used%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Data Footprint</td>
<td>16.84GB</td>
<td>1%</td>
</tr>
<tr>
<td>Footprint in Performance Tier</td>
<td>131.7MB</td>
<td>1%</td>
</tr>
<tr>
<td>Footprint in my-bucket</td>
<td>16.74GB</td>
<td>99%</td>
</tr>
<tr>
<td>Volume Guarantee</td>
<td>0B</td>
<td>0%</td>
</tr>
<tr>
<td>Flexible Volume Metadata</td>
<td>429.1MB</td>
<td>0%</td>
</tr>
<tr>
<td>Delayed Frees</td>
<td>27.60MB</td>
<td>0%</td>
</tr>
<tr>
<td>Total Footprint</td>
<td>17.29GB</td>
<td>1%</td>
</tr>
</tbody>
</table>
```

Available License Capacity

A capacity warning is triggered when the cloud tier reaches 85% of the maximum capacity set by the capacity-based license. Tiering to the cloud tier stops when the amount of data (used capacity) stored on the third-party cloud tier reaches the licensed capacity. Additional data, including SnapMirror copies to volumes using the All tiering policy, cannot be tiered until the license capacity is increased. Although tiering stops, data remains accessible from the cloud tier. Cold data remains on SSDs until the licensed capacity is increased.

To view the capacity status of the FabricPool license using the ONTAP CLI, run the following command:

```
system license show-status
```
Example:

<table>
<thead>
<tr>
<th>system license show-status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>valid</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>not-installed</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>not-applicable</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

To view the capacity status of the FabricPool license using ONTAP System Manager, complete the following steps:

1. Click CLUSTER.
2. Click Settings.
3. Click FabricPool License.
4. Current capacity is listed in the Current Capacity column.

Figure 19) License capacity.

<table>
<thead>
<tr>
<th>OWNER</th>
<th>STATE</th>
<th>SERIAL NUMBER</th>
<th>CAPACITY (AVAILABLE %</th>
<th>TOTAL)</th>
<th>EXPIRATION DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>aff</td>
<td>Compliant</td>
<td>360000104</td>
<td>99%</td>
<td>1TB</td>
<td>n/a</td>
</tr>
</tbody>
</table>

7.5 Virtualized Object Storage

Do not host virtualized object stores, (sometimes referred to as bare metal object storage) in volumes that tier inactive data. Set the tiering policy on those volumes to None.

Failure to set the tiering policy to None can place the virtualized object store at risk as blocks associated with the virtual machines may be marked as cold and tiered into themselves, causing significant spikes in latency and reductions in throughput when read.
8 Data Tiering Within Cloud Volumes ONTAP

Data Tiering within Cloud Volumes ONTAP is based on FabricPool technology; however, it has different advantages and limitations.

Data Tiering within the Cloud Volumes ONTAP documentation is now located on the NetApp Cloud Docs site:

- Data Tiering with Cloud Volumes ONTAP: Data Tiering Overview
- Data Tiering with Cloud Volumes ONTAP: Tiering Inactive Data to Low-Cost Object Storage
- Data Tiering with Cloud Volumes ONTAP: Cloud Manager and Cloud Volumes ONTAP documentation

9 Cloud Tiering Service

The Cloud Tiering Service is based on FabricPool technology; however, it has different advantages and limitations.

Cloud Tiering Service documentation is located on the NetApp Cloud Central site:

- Cloud Tiering with Cloud Volumes ONTAP

10 NetApp Private Storage for AWS

NetApp Private Storage (NPS) for AWS meets or exceeds all FabricPool best practices. The NPS for AWS solution is a high-performance cloud-connected storage architecture that allows enterprises to build an agile cloud infrastructure that combines the scalability and flexibility of the AWS cloud with the control and performance of NetApp storage.

NPS for AWS is typically deployed at one of the many AWS-approved Direct Connect partner colocation data centers (for example, Equinix). It uses AWS Direct Connect to provide a low-latency, highly available, dedicated connection between NetApp storage and the AWS cloud.
Where to Find Additional Information

To learn more about the information that is described in this document, review the following documents and/or websites:

- ONTAP System Manager
  http://docs.netapp.com/us-en/ontap/index.html
- Commands: ONTAP 9.7 Manual Page Reference
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-cmpr-970/home.html
- Configuring StorageGRID certificates for ONTAP clients using FabricPool
- ONTAP 9 Disks and Aggregates Power Guide
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-psmg/home.html
- ONTAP 9 Documentation Center
  https://docs.netapp.com/ontap-9/index.jsp
- ONTAP and ONTAP System Manager Documentation Resources page
- ONTAP FabricPool Licensing Overview
  https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_OS/ONTAP_FabricPool_(FP)_Licensing_Overview
- StorageGRID Administrator Guide
- TR-4015: SnapMirror Configuration and Best Practices Guide
- TR-4075: DataMotion for Volumes
- TR-4133: NetApp Private Storage for Amazon Web Services (AWS)
- TR-4375: NetApp MetroCluster FC
- TR-4571: FlexGroup Volume Best Practices
- TR-4626: StorageGRID Load Balancer Options
- TR-4689: NetApp MetroCluster IP
- TR-4695: Database Storage Tiering with FabricPool
- TR-4826: FabricPool with StorageGRID
- NVA-0009: NetApp Private Storage for Cloud
### Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2</td>
<td>January 2020</td>
<td>John Lantz: Updated for ONTAP 9.7. Support for FabricPool Mirror, MetroCluster, S3-compatible providers, and NDMP. Writes from the cloud tier to the local tier are now disabled if local tier capacity is greater than 90%. Major updates to System Manager interfaces. NetApp terminology now refers to aggregates as local tiers.</td>
</tr>
<tr>
<td>2.1</td>
<td>September 2019</td>
<td>John Lantz: Added details regarding the All tiering policy.</td>
</tr>
<tr>
<td>1.9</td>
<td>March 2019</td>
<td>John Lantz: Added details regarding AES-256-GCM encryption and the need to avoid clock skew when attaching to private clouds.</td>
</tr>
<tr>
<td>1.8</td>
<td>January 2019</td>
<td>John Lantz: Updated for ONTAP 9.5. Added support for FlexGroup volumes, client-side encryption, Amazon Commercial Cloud Services (C2S), IBM Cloud Object Storage, and the ability to change the aggregate fullness threshold. Aggregated Storage Tiering with Cloud Volumes ONTAP information.</td>
</tr>
<tr>
<td>1.7</td>
<td>August 2018</td>
<td>John Lantz: Added additional information regarding Cloud Volumes ONTAP capacity and performance.</td>
</tr>
<tr>
<td>1.6</td>
<td>July 2018</td>
<td>John Lantz: Cloud ONTAP renamed to Cloud Volumes ONTAP. Added additional information regarding metadata.</td>
</tr>
<tr>
<td>1.5</td>
<td>June 2018</td>
<td>John Lantz: Support for tiering to Microsoft Azure Blob Storage, the Auto volume tiering policy, and io1 EBS volumes added to ONTAP Cloud. Writes from the cloud tier to the performance tier are disabled if performance tier capacity is greater than 70%.</td>
</tr>
<tr>
<td>1.4</td>
<td>May 2018</td>
<td>John Lantz: Updated for ONTAP 9.4. Added Auto tiering policy, Microsoft Azure Blob support, inactive data reporting, and support for ONTAP Select Premium.</td>
</tr>
<tr>
<td>1.3</td>
<td>January 2018</td>
<td>John Lantz: Updated for ONTAP 9.3. Added ONTAP Cloud functionality, AWS GovCloud S3, and additional interoperability details (QoS, StorageGRID, etc.).</td>
</tr>
<tr>
<td>1.2</td>
<td>September 2017</td>
<td>John Lantz: Added details regarding connectivity requirements.</td>
</tr>
<tr>
<td>1.1</td>
<td>August 2017</td>
<td>John Lantz: Added details regarding intercluster LIF requirements.</td>
</tr>
</tbody>
</table>
Contact Us

Let us know how we can improve this technical report.
Contact us at doccomments@netapp.com.
Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer’s installation in accordance with published specifications.

Copyright Information

Copyright © 2019–2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

TR-4598-0707