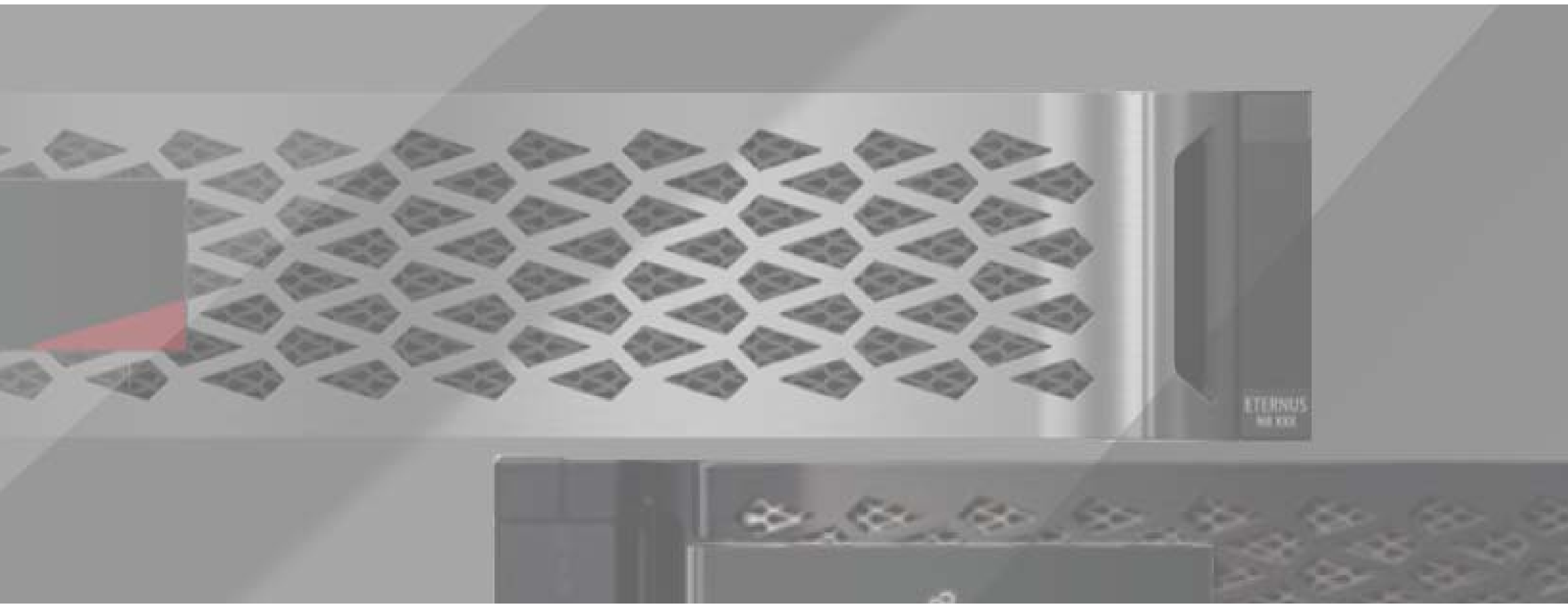
P3AG-6642-02ENZ0

Fujitsu Storage ETERNUS AX series All-Flash Arrays, ETERNUS HX series Hybrid Arrays

S3 in ONTAP Best Practices ONTAP 9.13.1



FUJITSU

Table of Contents

List of Figures

List of Tables

Preface

This document describes best practices for using the Amazon Simple Storage Service (S3) with ONTAP software. We also cover capabilities and configurations for using ONTAP as an object store with native S3 applications or as a tiering destination for FabricPool.

Second Edition
November 2023

Trademarks

Third-party trademark information related to this product is available at:
https://www.fujitsu.com/global/products/computing/storage/eternus/trademarks.html

Trademark symbols such as ™ and ® are omitted in this document.

About This Manual

Intended Audience

This manual is intended for system administrators who configure and manage operations of the ETERNUS AX/HX, or field engineers who perform maintenance. Refer to this manual as required.

Related Information and Documents

The latest information for the ETERNUS AX/HX is available at:
https://www.fujitsu.com/global/support/products/computing/storage/manuals-list.html

Document Conventions

- Notice Symbols

The following notice symbols are used in this manual:

Caution — Indicates information that you need to observe when using the ETERNUS AX/HX. Make sure to read the information.

Note — Indicates information and suggestions that supplement the descriptions included in this manual.

1. Overview

Beginning in ONTAP 9.8, ONTAP software supports the Amazon Simple Storage Service (S3). ONTAP supports a subset of AWS S3 API actions and allows data to be represented as objects in an ONTAP-based ETERNUS AX/HX system.

2. Primary Use Cases

The primary purpose of S3 in ONTAP is to provide support for objects on ONTAP-based systems. The ONTAP unified storage architecture now supports files (NFS and SMB), blocks (FC and iSCSI), and objects (S3).

Native S3 Applications

An increasing number of customers need ONTAP to support objects using S3. Although well suited for high-capacity archival workloads, demand for native S3 applications is growing rapidly and includes:

- Analytics
- Artificial intelligence
- Edge-to-core ingest
- Machine learning

Customers can now use familiar manageability tools such as ONTAP System Manager to rapidly provision high-performance object storage for development and operations in ONTAP, taking advantage of the ONTAP storage efficiencies and security as they do so.

Beginning with ONTAP 9.12.1, the S3 protocol can also be enabled in multiprotocol NAS volumes that have been preconfigured to use NAS protocols. When the S3 protocol is enabled in multiprotocol NAS volumes, client applications can read and write data using S3, NFS, and SMB, which opens up a variety of additional use cases. One of the most common use cases is NAS clients writing data to a volume and S3 clients reading the same data and performing specialized tasks such as analytics, business intelligence, machine learning, and optical character recognition.

FabricPool Endpoints

Beginning with ONTAP 9.8, FabricPool supports tiering to buckets in ONTAP, allowing for ONTAP to ONTAP tiering. This is an excellent option for customers who wish to repurpose existing ETERNUS AX/HX infrastructure as an object store endpoint.

FabricPool supports tiering to ONTAP in two ways:

- **Local cluster tiering**
  Inactive data is tiered to a bucket located on the local cluster using cluster LIFs.

- **Remote cluster tiering**
  Inactive data is tiered to a bucket located on a remote cluster similarly to a traditional FabricPool cloud tier using inter-cluster LIFs on the FabricPool client and data LIFs on the ONTAP object store.

Fujitsu recommends using StorageGRID or FJcloud-o, the premier object store solution, when tiering more than 300TB of inactive data. A FabricPool license is not required when using ONTAP, StorageGRID, or FJcloud-o as the cloud tier.

3. Requirements

Platforms

- **ETERNUS AX series**
  S3 is supported on all ETERNUS AX platforms using ONTAP 9.8+.
- **ETERNUS HX series**
  S3 is supported on all ETERNUS HX platforms using ONTAP 9.8+.
- **Cloud Volumes ONTAP**
  - S3 is supported on Cloud Volumes ONTAP for Azure and Cloud Volumes ONTAP for FUJITSU Hybrid IT Service for Microsoft Azure using ONTAP 9.9+.
  - S3 is supported on Cloud Volumes ONTAP for AWS and Amazon FSx for NetApp ONTAP using ONTAP 9.11+.
  - S3 is supported on Cloud Volumes ONTAP for Google Cloud using ONTAP 9.12+.

Data LIFs

Storage virtual machines (SVMs) hosting object store servers require data LIFs to communicate with client applications using S3. When configured for remote cluster tiering, FabricPool is the client and the object store is the server.

Cluster LIFs

When configured for local cluster tiering, a local tier (also known as a storage aggregate in the ONTAP CLI) is attached to a local bucket. FabricPool uses cluster LIFs for intracluster traffic.

> **Caution**
>
> Performance degradation might occur if cluster LIFs resources become saturated. To avoid this, Fujitsu recommends using four-node, or greater, clusters when tiering to a local bucket—the recommended best practice being an HA pair for the local tier and an HA pair for the local bucket. Tiering to local buckets on single HA pair is not recommended.

S3 License

As with other protocols such as FC, iSCSI, NFS, NVMe_oF, and SMB, S3 requires the installation of a license before it can be used in ONTAP. The S3 license is a zero-cost license, but it must be installed on systems upgrading to ONTAP 9.8.

New ONTAP 9.8 systems have the S3 license pre-installed.

Installation

To install the S3 license, run the following command in the ONTAP CLI:

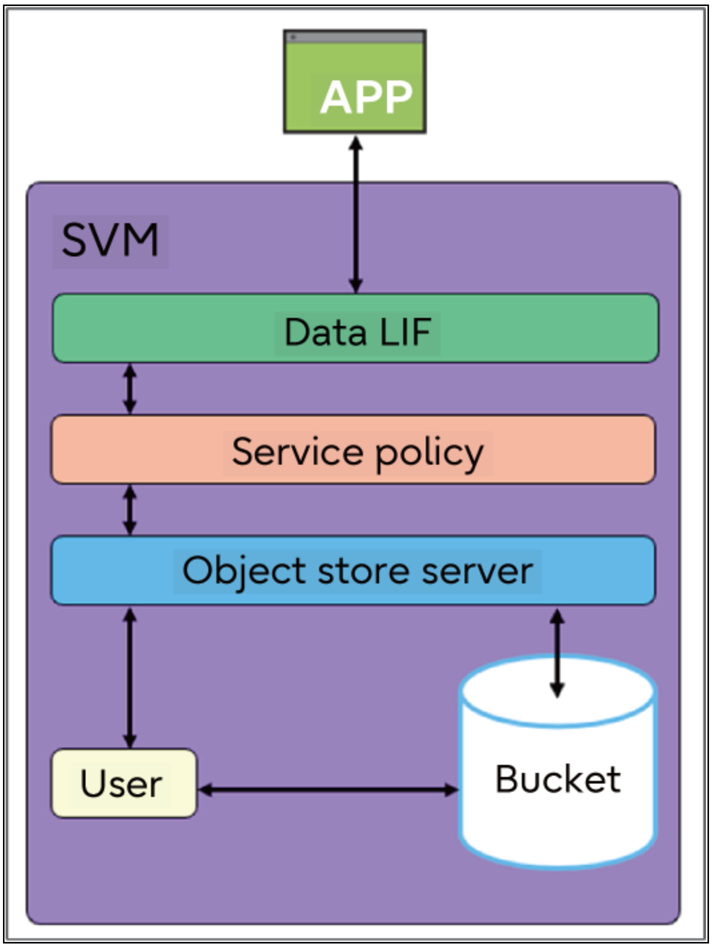
```
system license add <license_key>
```

4. Architecture

Object storage is an 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 might be less performative than file or block storage, it is significantly more scalable, and buckets containing petabytes of data are not uncommon.

Figure 1 The Core Elements of an S3 Object Storage in ONTAP



Service Policy

Data service policies are assigned to SVMs and provide a collection of network services required by data LIFs to support client application protocols. For example, data-nfs is used to support NFS traffic, data-iscsi is used to support iSCSI traffic, and so on.

New in ONTAP 9.8, the data-s3-server service, allows data LIFS to support client application traffic using S3.

Note

In addition to the data-s3-server service, the data-core service should be included in any service policy to make sure that applications using the LIF work as expected.

Object Store Server

The SVM's object store server manages data as objects, as opposed to other storage architectures such as file or block storage. Management of bucket and user permission levels also takes place at the object store server level.

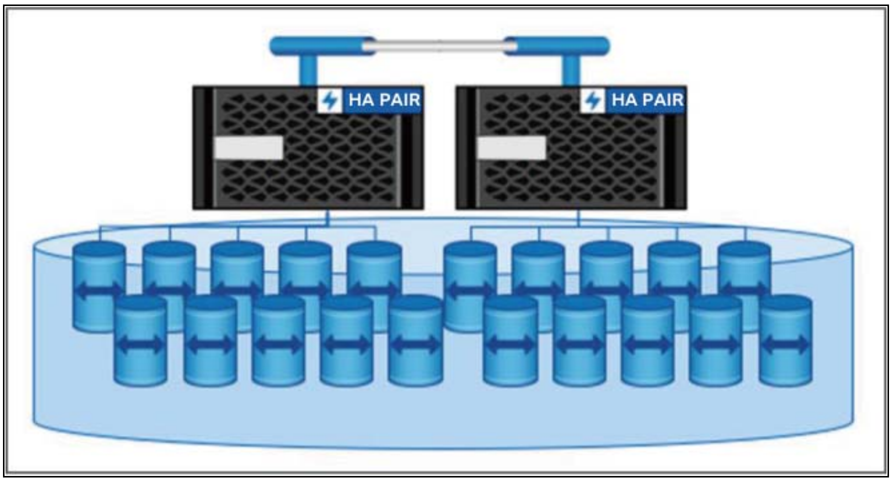
ONTAP S3 supports one object store server per SVM.

Bucket

In ONTAP, the underlying architecture for a bucket is a FlexGroup volume—a single namespace that is made up of multiple constituent member volumes but is managed as a single volume, as shown in Figure 2. Individual objects in a bucket are allocated to individual member volumes and are not striped across volumes or nodes. Individual buckets cannot be provisioned smaller than 96GB.

For more information about FlexGroup volumes, refer to "Technical Overview of ONTAP FlexGroup Volumes" in Fujitsu manual site.

Figure 2 FlexGroup Volume



When used by buckets, FlexGroup volumes use elastic sizing, not volume autogrow. FlexGroup volume maximums are only limited by the physical maximums of the underlying hardware and have been tested to 20PB and 400 billion files in a 10-node cluster.

ONTAP S3 supports up to 12,000 buckets, although no more than 1,000 buckets should be created on a single FlexGroup volume.

The Amazon S3 maximum object size is 5TB. ONTAP S3 supports objects up to 16TB. Objects greater than 5TB might result in interoperability issues for clients that cannot exceed Amazon-defined maximum object sizes.

Note

Underlying architectural changes between ONTAP 9.7 (one bucket per FlexGroup volume) and ONTAP 9.8 or later (multiple buckets per FlexGroup volume) cannot be made in place. Data must be migrated from preexisting buckets to ONTAP 9.8 or later buckets to take advantage of the new architecture.

Default Bucket Settings

Buckets that are not manually configured use default settings for aggregate, FlexGroup, and bucket provisioning.

Aggregates

FlexGroup volumes supporting buckets are provisioned on aggregates by using the following priorities:

- Flash Pool aggregate
- HDD aggregate
- SSD aggregate

FlexGroup volumes

The default FlexGroup size is large and provides significant room for expansion in most environments:

- 1.6PB in ONTAP

If a cluster does not have enough capacity to provision the default size, the size is reduced by half until it can be provisioned in the existing environment. For example, in a 300TB environment, a FlexGroup volume is automatically provisioned at 200TB (1.6PB, 800TB, and 400TB FlexGroup volumes being too large for the environment).

Buckets

The default bucket size is:

- 800GB in ONTAP

To provide capacity for bucket expansion, the total capacity of all buckets on the FlexGroup volume should be less than 33% of the FlexGroup volume capacity. If this cannot be met, the bucket being created is automatically provisioned on a newly created FlexGroup volume.

Users

User authorization is required on all ONTAP object stores to restrict connectivity to authorized clients. Access to specific buckets or S3 actions can be allowed, denied, or made conditional at the user level.

ONTAP S3 supports 4,000 users per object store.

S3 in Multiprotocol NAS Volumes

When S3 is used in multiprotocol NAS volumes (ONTAP 9.12.1+), it is mapped to existing NAS hierarchies. For example, buckets are mapped to a volume or a directory inside a volume. NAS security configurations, including file, directory, and user permissions, are preserved and mapped to S3 users in the same way that NFS and SMB configurations are mapped to each other.

Objects are mapped to files and are presented to S3 clients using a naming scheme based on the underlying NAS hierarchy with folder/object corresponding to directory/file.

Caution

Because the underlying architecture is file-based, not object-based, S3 in multiprotocol NAS volumes imposes NAS-related limits that might not exist when using native S3. For example, file and directory names are limited to 255 characters and 1024-byte paths, so corresponding object names are limited to 255 characters and 1024 bytes as well.

5. Configuration for Native S3 Applications and Remote Cluster Tiering

External clients such as native S3 applications and FabricPool clients connect to the ONTAP object store using data LIFs. The easiest way to create an object store in ONTAP is by using ONTAP System Manager. Processes that require multiple steps when using the CLI are reduced to a few clicks using Fujitsu recommended best practices. Configuration with the CLI is required for more custom configurations.

ONTAP System Manager

To create an object store, bucket, and permission, users using ONTAP System Manager must complete the following steps:

Configure the Object Store

To configure the object store, complete the following steps:

Procedure ▶▶▶

1 Launch ONTAP System Manager.

2 Click **STORAGE**.

3 Click **Storage VMs**.

4 Click **Add**.

A new SVM is not necessary. S3 functionality can be added to existing SVMs using the SVM's **Settings** menu.

5 Name the SVM.

6 Select **Enable S3** as an access protocol.

The options **Enable TLS (port 443)** and **Use System-Generated Certificate** are selected by default. Using signed certificates from a third-party certificate authority is a recommended best practice.

7 Name the S3 server.

> **Note**
>
> The server name is used as the fully qualified domain name (FQDN) by client applications.

8 Enter network interfaces for the nodes.

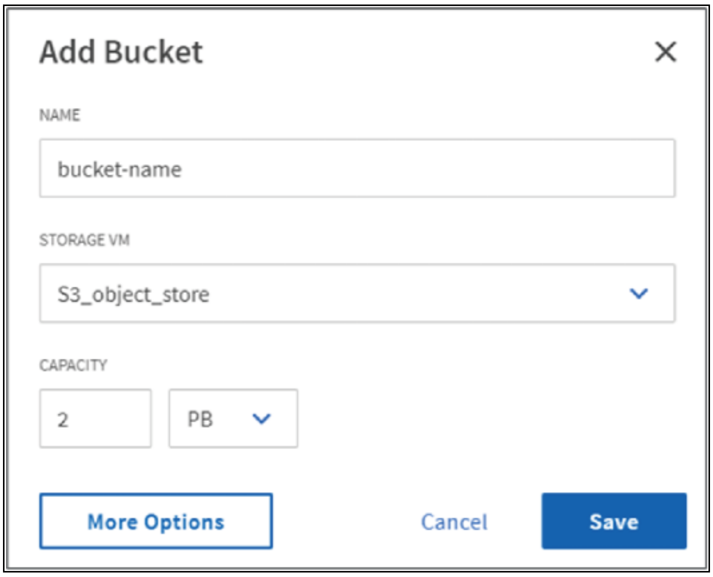
◀◀◀

Configure a Bucket

To configure a bucket, complete the following steps:

Procedure ▶▶▶

1. Launch ONTAP System Manager.
2. Click **STORAGE**.
3. Click **Buckets**.
4. Click **Add**.
5. Name the bucket.
6. Select the SVM/object store that the bucket will be assigned to. This should be the same SVM/object store created earlier.
7. Click **Save**.



Add Bucket

NAME: bucket-name

STORAGE VM: S3_object_store

CAPACITY: 2 PB

◀◀◀

More Options

Use for tiering

If you select this option, ONTAP System Manager creates the bucket on the least expensive media, prioritizing HDD > SSD > NVMe.

Performance service level

Select the appropriate quality of service (QoS) for the bucket. Options include:

- **Extreme**
  50,000 IOPS; 1562MBps
- **Performance**
  30,000 IOPS; 937MBps
- **Value**
  15,000 IOPS; 468MBps
- **Custom**
  Use an existing QoS policy or create a new one.

> **Note**
>
> Performance service levels are not selectable if the bucket is used for tiering. FabricPool does not support QoS minimums.

Permissions

Copy access permissions from an existing bucket or create new ones.

> **Note**
>
> Users and groups must be configured before they can be permissioned. See "Add Users and Groups" (page 19).

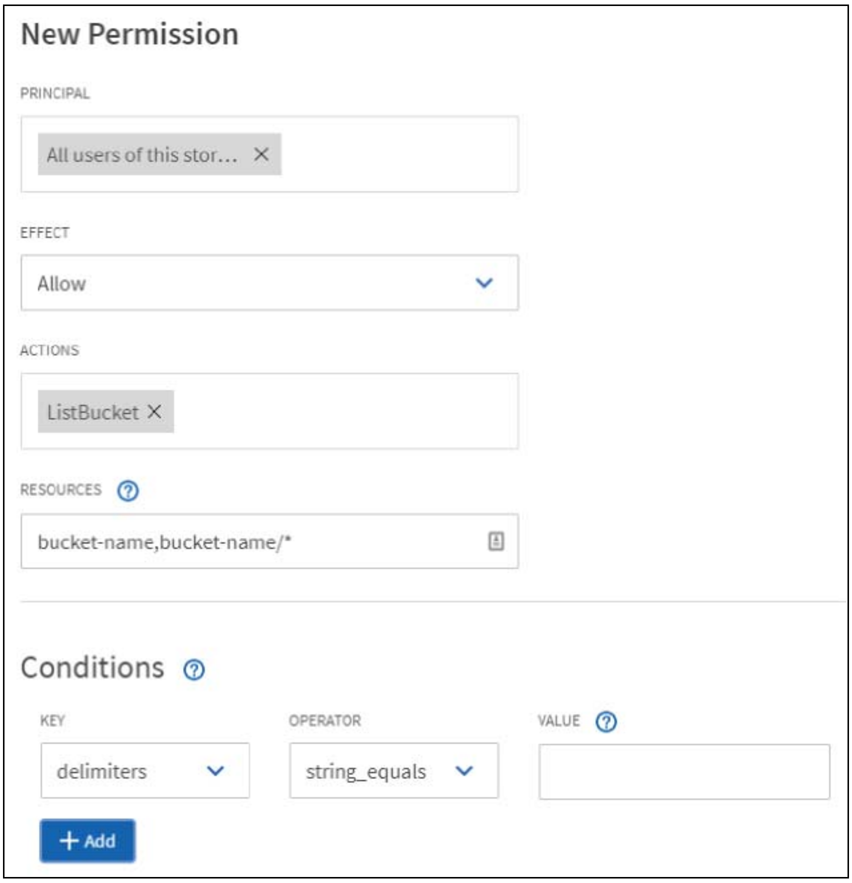
To create new permissions, complete the following steps:

Procedure ▶▶▶

1. From the Add Bucket page, scroll down to **Permissions** and click **Add**.
2. Set principal users.
   Options include All users of the SVM (default), All public and anonymous users, and individual users associated with the SVM.
3. Set effect.
   Options include Allow (default) and Deny.
4. Set actions.
5. Set resources.
   "bucket-name" and "bucket-name/*" are used by default.
6. Set conditions.

7 Add conditions.

Up to 10 conditional statements can be added. Each conditional statement is composed of a key, an operator, and one or more values.



New Permission

PRINCIPAL: All users of this stor…

EFFECT: Allow

ACTIONS: ListBucket

RESOURCES: bucket-name,bucket-name/*

Conditions

KEY: delimiters

OPERATOR: string_equals

VALUE:

Add Users and Groups

User authorization is required on all ONTAP object stores to restrict connectivity to authorized clients. Access to specific buckets or S3 actions can be allowed, denied, or made conditional at the user and group level using permissions.

ONTAP S3 supports 4000 users per object store or SVM.

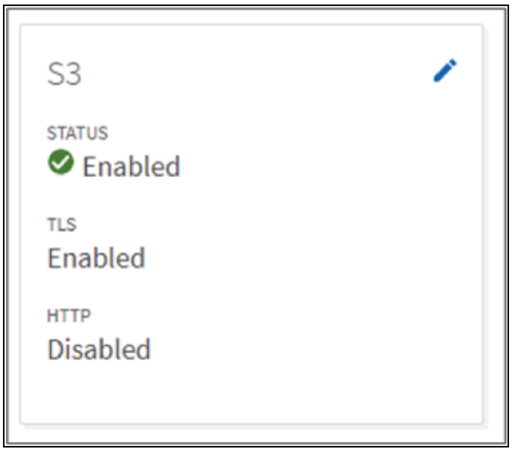
Note

A root user (UID 0) is created by default when the bucket is created. The root user has full access to all buckets and objects. Do not use the root user for client application access. Additional users must be created for client access.

To manage users and groups, complete the following steps:

Procedure ▶▶▶

1. Launch ONTAP System Manager.
2. Click **Storage**.
3. Click **Storage VMs**.
4. Select the SVM to add users and groups to.
5. Click the **Edit** icon on the S3 protocol box.



S3

STATUS
✓ Enabled

TLS
Enabled

HTTP
Disabled

6. Select the **Users or Groups** tab.
7. Click **Add**.
8. Name the user or group.
9. Copy and/or download the access and secret key for future use.

> **Note**
>
> The secret key is not displayed again.

10. If you are configuring a group, assign users and policies.
11. If you are configuring a user, use the permissions menu.

◀◀◀

ONTAP CLI

Although the easiest way to create an object store in ONTAP is by using the ONTAP System Manager, object stores created using ONTAP System Manager allow for less customization.

For example, ONTAP System Manager automatically selects the local tiers (aggregates) use by a bucket for storage. Although it uses recommended best practices to do so, for complex environments, the selected local tiers might not be the same ones an experienced storage administrator would use.

Configuration using the ONTAP CLI is required for custom configurations.

To create an object store, bucket, and permission users using ONTAP CLI, complete the following steps:

Procedure

1. Create the service policy.
2. Create a data LIF to use S3.
3. Install a CA certificate.
4. Create the object store server.
5. Create the bucket.
6. Create a user.

Create the Service Policy

A service policy is required to enable S3 data traffic on the SVM LIFs.

To create the service policy by using the ONTAP CLI, run the following command:

```
network interface service-policy create
-vserver <name>
-policy <name>
-services data-s3-server, data-core
```

Note

In addition to the data-s3-server service, the data-core service should be included in any service policy to make sure that applications using the LIF work as expected.

Create a Data LIF to Use with S3

SVMs hosting object store servers require data LIFs to communicate with client applications using S3. Fujitsu recommends creating an S3 data LIF on all nodes as a best practice.

When configured for remote cluster tiering, FabricPool is the client and the object store is the server. Because FabricPool requires the object store to use an FQDN, all S3 DATA LIFs must be associated with the FQDN used by the Object Store Server.

Note

Creation of the DNS entry is external to ONTAP. Fujitsu recommends creating a single host entry that uses all S3 data LIF IP addresses.
The `dns-zone` setting is for ONTAP DNS load balancing.

To create a LIF to use the service policy using the ONTAP CLI, run the following command:

```
network interface create
-vserver <name>
-lif <name>
-service-policy <name>
-home-node <node>
-home-port <port>
-address <number>
-netmask <number>
-status-admin up
```

Install a CA Certificate

Using CA certificates creates a trusted relationship between client applications and the ONTAP object store server. A CA certificate should be installed on ONTAP before using it as an object store that is accessible to remote clients.

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

To install a CA certificate using the ONTAP CLI, run the following command:

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

Create the Object Store Server

The ONTAP object store server manages data as objects, as opposed to other storage architectures such as file or block storage.

To create an object store server using the ONTAP CLI, run the following command:

```
vserver object-store-server create
-vserver <name>
-object-store-server <FQDN>
-certificate-name <name>
-secure-listener-port <443>
-is-http-enabled <false>
```

Note

FabricPool must resolve this name to all IP addresses used by S3 data LIFs through DNS.

Create a User

User authorization is required on all ONTAP object stores to restrict connectivity to authorized clients.

Note

All S3 users with valid access and a secret key-pair can access all buckets and objects in the SVM.

To create a user by using the ONTAP CLI, run the following command:

```
vserver object-store-server user create
-vserver <name>
-user <name>
```

To view the user’s access and secret key by using the ONTAP CLI, run the following command:

Note

Advanced privilege level is required.

```
object-store-server user show
```

Root User

A root user (UID 0) is created by default when the bucket is created. The root user has full access to all buckets and objects. Do not use the root user for client application access. Additional users must be created for client access.

The ONTAP administrator must run the `object-store-server users regenerate-keys` command to set the access key and secret key for this user.

Create the Bucket

To create a bucket using the ONTAP CLI, run the following command:

```
vserver object-store-server bucket create
-vserver <name>
-bucket <name>
-type s3
-used-as-capacity-tier <true|false>
-aggr-list <aggregate name>, <aggregate name> (option for non-capacity tier)
-exclude-aggr-list <aggregate name>, <aggregate name> (option for capacity tier)
-aggr-list-multiplier <number of constituent volumes per aggregate> (default 4)
-size <size>
```

Beginning with ONTAP 9.11.1, ONTAP S3 supports bucket versioning. Enabling versioning allows for the creation of multiple versions of an object. Much like Snapshot copies, these objects can be retrieved and restored, enabling client applications to restore deleted objects or retrieve earlier versions of an object.

To create a bucket using the ONTAP CLI, run the following command:

```
vserver object-store-server bucket modify
-vserver <name>
-bucket <name>
-versioning-state <disabled|enabled|suspend>
```

Note

The default versioning state is "disabled".

6. Configuration for Local Cluster Tiering

Beginning with ONTAP 9.8, FabricPool supports tiering to buckets in ONTAP, allowing for ONTAP-to-ONTAP tiering. This is an excellent option for customers who wish to repurpose existing ETERNUS AX/HX infrastructure as an object store endpoint.

When configured for local cluster tiering, inactive data is tiered from local aggregates (typically SSD) to a local bucket (typically HDD) using cluster LIFs.

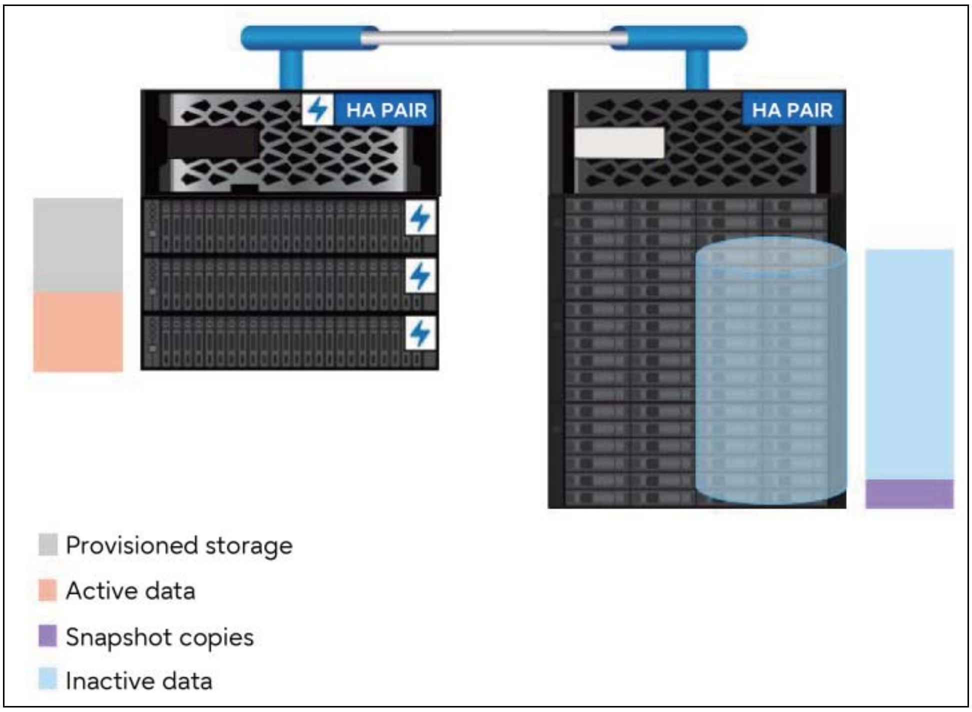
Fujitsu recommends using StorageGRID, the premier Fujitsu object store solution, when tiering more than 300TB of inactive data. A FabricPool license is not required when using ONTAP or StorageGRID as the cloud tier.

For more information on FabricPool, see "FabricPool Best Practices" in Fujitsu manual site.

Caution

Performance degradation might occur if cluster LIFs resources become saturated. To avoid this, Fujitsu recommends using two-node, or greater, clusters when tiering to a local bucket—the recommended best practice being an HA pair for the local tier and an HA pair for the local bucket. Tiering to local buckets on single-node clusters is not recommended.

Figure 3 Local Cluster Tiering



ONTAP System Manager

The easiest way to create an object store for local tiering in ONTAP is by using ONTAP System Manager, which reduces multiple steps when using the CLI to a few clicks. Object stores created using ONTAP System Manager allow for less customization but use Fujitsu recommended best practices by default. Configuration via the CLI is required for custom configurations.

Configure the Object Store

To create an object store used for local cluster tiering, complete the following steps:

Procedure ▶▶▶

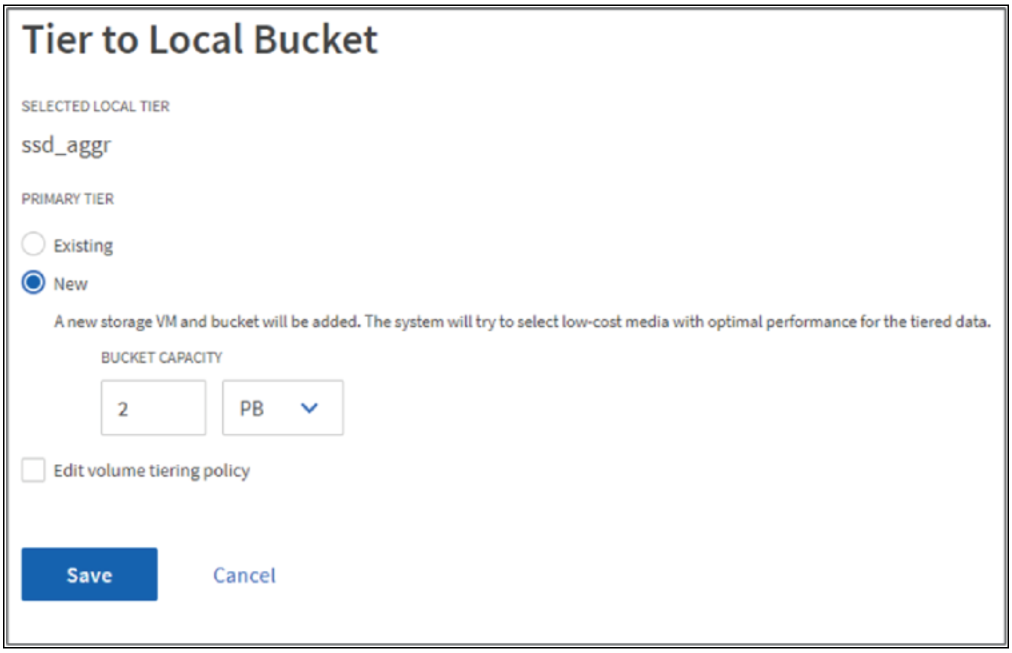
1. Launch ONTAP System Manager.
2. Click **Storage**.
3. Click **Tiers**.
4. Select a local tier.
5. Click **More**.
6. Select **Tier to Local Bucket**.
7. Select **New** if this is the first local bucket on the system.

   A new SVM, object store server, and bucket are created. ONTAP System Manager creates the bucket on the least expensive media, prioritizing HDD > QLC > TLC > NVMe.

   Select **Existing** if a local bucket has already been created.

   Note

   Attaching the same local bucket to all local FabricPool tiers in the cluster enables optimized volume moves. 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. Optimized volume moves result in significant network efficiencies.



Tier to Local Bucket

SELECTED LOCAL TIER

ssd_aggr

PRIMARY TIER

○ Existing

● New

A new storage VM and bucket will be added. The system will try to select low-cost media with optimal performance for the tiered data.

BUCKET CAPACITY

2 PB

□ Edit volume tiering policy

8. Set bucket capacity.
9. Edit volume tiering policies (optional).
10. Click **Save**.

ONTAP CLI

Although the easiest way to create an object store for local tiering in ONTAP is by using ONTAP System Manager, object stores created using ONTAP System Manager allow for less customization.

For example, ONTAP System Manager automatically selects the local tiers (aggregates) used by a bucket for storage. Although ONTAP System Manager uses recommended best practices to do so, for complex environments, the selected local tiers might not be the same ones an experienced storage administrator would select.

Configuration using the ONTAP CLI is required for custom configurations.

To create an object store and bucket for local tiering using ONTAP CLI, complete the following steps:

Procedure

1. Create the object store server on the Cluster SVM.
2. Create a bucket on a data SVM.
3. Create a user.
4. Add a cloud tier using the object store and bucket.

5 Attach the cloud tier to a local tier.

Create the Object Store Server on the Cluster SVM

To create an object store server on the Cluster SVM using the ONTAP CLI, run the following command:

```
vserver object-store-server create
-vserver Cluster
-object-store-server <name> (This is the FGDN used by FabricPool)
-is-http-enabled true
-is-https-enabled false
-status-admin up
```

Although installation and use of certificate authority (CA) certificates are recommended best practices, installation of CA certificates is not required when tiering locally. If you are not using a certificate, HTTP must be enabled and HTTPS must be disabled:

- ### Set object-store permissions

Permissions can be set at the object store level that apply to all (or specified) buckets in the object store. To set an object store policy statement using the ONTAP CLI, run the following command:

```
vserver vserver object-store-server policy statement create
-vserver <data svm>
-policy <name>
-effect <allow/deny>
-action <*, GetObject, PutObject, DeleteObject, ListBucket, etc.>
-principal <S3 user or group> (maximum of 10 per policy)
-resource <bucket name>
```

Create a Bucket on a Data SVM

To create a bucket using the ONTAP CLI, run the following command:

```
vserver object-store-server bucket create
-vserver <name>
-bucket <name>
-type s3
-used-as-capacity-tier true
-exclude-aggr-list <aggregate name>,<aggregate name>
-aggr-list-multiplier <number of constituent volumes per aggregate> (default 4)
-size <size> (95GB minimum)
```

Note

Advanced privileges are required to use `-aggr-list`.

- ### Set bucket permissions

To set a bucket permission statement using the ONTAP CLI, run the following command:

```
vserver vserver object-store-server bucket policy add-statement
-vserver <data svm>
-bucket <name>
-effect <allow/deny>
-action <*, GetObject, PutObject, DeleteObject, ListBucket, etc.>
-principal <S3 user or group> (maximum of 10 per policy)
-resource <bucket name, bucket-name/*>
```

Note

To add anonymous access, a principal must be configured as *.

Create a User

User authorization is required on all ONTAP object stores to restrict connectivity to authorized clients.

Note

All S3 users with valid access and a secret key pair can access all buckets and objects in the SVM.

To create a user by using the ONTAP CLI, run the following command:

```
vserver object-store-server user create
-vserver <name>
-user <name>
```

To view the user's access and secret key by using the ONTAP CLI, run the following command:

Note

Advanced privilege level is required.

```
object-store-server user show
```

- ### User groups

A user can be added to groups that can be associated with policy statements at the object store level or the bucket level. To create a group policy and add users to it using the ONTAP CLI, run the following command:

```
vserver vserver object-store-server group create
-vserver <data svm>
-name <group name>
-users <user1, user2, etc.
-policy <policy name>
```

Add a Cloud Tier Using the Object Store and Bucket

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

```
storage aggregate object-store config create
-object-store-name <name the cloud tier>
-provider-type ONTAP_S3
-server <name of the Cluster svm object store server>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ipspace Cluster
-ssl-enabled <true/false>
-is-certificate-validation-enabled true
-use-http-proxy false
-url-stle <path-style/virtual-hosted-stle>
```

Attach the Cloud Tier to a Local Tier

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

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

Caution

Attaching a local bucket to a local tier is a permanent action. A local bucket cannot be unattached from a local tier after being attached.

7. Configuration for S3 in Multiprotocol NAS Volumes

Beginning in ONTAP 9.12.1, S3 can be enabled in pre-existing NAS volumes that have been fully configured to serve NFS or SMB clients. Enabling the S3 protocol on a volume that supports NFS and/or SMB but has not been configured to serve data to does not work. ONTAP must be able to map S3 users to pre-existing users created with Unix or Windows security styles. Enabling S3 on a NAS volume that has not been configured to serve NFS or SMB clients does not work.

To enable NAS protocols, see the following resources:

- Provision NAS storage for Linux servers using NFS
- Provision NAS storage for Windows servers using SMB

Caution

Multiprotocol NAS volumes are NAS volumes that present NAS hierarchies and files as buckets and objects. Actions and capabilities associated with metadata, multipart objects, tags, and versioning are not supported when using S3 in multiprotocol NAS volumes. Clients that require these actions and capabilities should use native ONTAP S3.

ONTAP System Manager

The easiest way to enable S3 in a multiprotocol NAS volume in ONTAP is by using the ONTAP System Manager; this reduces the multiple steps needed with the CLI to a few clicks. Object stores created using ONTAP System Manager allow for less customization, but they are created with Fujitsu recommended best practices by default. Configuration with the CLI is required for custom configurations.

To enable S3 in a multiprotocol NAS volume using ONTAP System Manager, complete the following steps:

Procedure ▶▶▶

1. Enable S3 on the SVM.
2. Create the bucket.
3. Enable name mapping.
4. Add bucket permissions.

◀◀◀

Enable S3 on the SVM

Procedure ▶▶▶

1. Launch ONTAP System Manager.
2. Click **Storage**.
3. Click **Storage VMs**.
4. Select a SVM configured to use NFS or SMB/CIFS protocols.
5. Click **Settings**.
6. Click the S3 gear icon.
7. Name the S3 server.

   Note

   The server name is used as the fully qualified domain name (FQDN) by client applications.

8. Select **Enable S3 as an access protocol**. The options **Enable TLS (port 443)** and **Use System-Generated Certificate** are selected by default. Using signed certificates from a third-party certificate authority is a recommended best practice.
9. Enter network interfaces for the nodes.

◀◀◀

Create the Bucket

Procedure ▶▶▶

1. Click **Storage**.
2. Click **Buckets**.
3. Click **Add**.
4. Name the bucket.
5. Select the SVM/object store that the bucket will be assigned to. This should be the same S3 server created on the multiprotocol SVM earlier. Clicking **More Options** allows you to map the bucket to a specific folder inside the volume.

   Note

   S3 buckets in multiprotocol NAS volumes cannot be used for tiering as FabricPool cloud tiers.

6. Click **Save**.

◀◀◀

Enable Name Mapping

User authorization is required on all ONTAP object stores to restrict connectivity to authorized clients. Access to specific buckets or S3 actions can be allowed, denied, or made conditional at the user and group level using permissions.

ONTAP S3 supports 4000 users per object store or SVM.

Caution

A root user (UID 0) is created by default when the bucket is created. The root user has full access to all buckets and objects. Do not use the root user for client application access. Additional users must be created for client access.

To manage users and groups, complete the following steps:

Procedure ▶▶▶

1. Click **Storage**.
2. Click **Storage VMs**.
3. Select the SVM to add users and groups to.
4. Click the **Settings** tab.
5. Click **Name Mapping**.
6. Select **S3 to Windows** or **S3 to Unix** (both can be used).
7. Click **Add**.
8. Select the pattern (S3) and replacement (Windows or Unix).

◀◀◀

Add Bucket Permissions

Copy access permissions from an existing bucket or create new ones.

Caution

Users and groups must be configured before they can be permissioned. See "Add Users and Groups" (page 19).

To create new permissions, complete the following steps:

Procedure ▶▶▶

1. Click **Storage**.
2. Click **Buckets**.
3. Select a bucket.
4. Click **Edit**.

5. Set principal users. Options include All users of the SVM (default), All public and anonymous users, and individual users associated with the SVM.
6. Set effect. Options include **Allow** (default) and **Deny**.
7. Set actions.
8. Set resources. bucket-name and bucket-name/* are used by default. NAS directories/folder paths can also be used.
9. Set conditions.
10. Add conditions. Up to 10 conditional statements can be added. Each conditional statement is composed of a key, an operator, and one or more values.

ONTAP CLI

To enable S3 in a multiprotocol NAS volume using ONTAP CLI, complete the following steps:

Procedure

1. Add the S3 service policy.
2. Verify the data LIF.
3. Install a CA certificate.
4. Create the object store server.
5. Create a bucket.
6. Enable name mapping.

Add the S3 Service Policy

An S3 service policy is required to enable S3 data traffic on the SVM LIFs.

To add the service policy by using the ONTAP CLI, run the following command:

```
network interface service-policy add-service
-vserver <name>
-policy <name>
-services data-s3-server
```

Note

S3 in multiprotocol volumes requires a pre-existing SVM configured to serve NAS data using data-core, and data-nfs, and/or data-cifs services.

Verify the Data LIF

SVMs hosting object store servers require data LIFs to communicate with client applications using NFS, SMB/CIFS, and S3. Fujitsu recommends using data LIFs on all nodes as a best practice.

Caution

Creation of the DNS entry is external to ONTAP. Fujitsu recommends creating a single host entry that uses all S3 data LIF IP addresses.
The `dns-zone` setting is for ONTAP DNS load balancing.

To verify the data LIF has already been configured to support client traffic, run the following command:

```
network interface show
-vserver <name>
```

Install CA Certificate

Using CA certificates creates a trusted relationship between client applications and the ONTAP object store server. A CA certificate should be installed on ONTAP before using it as object store that is accessible to remote clients.

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

To install a CA certificate using the ONTAP CLI, run the following command:

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

Create the Object Store Server

The ONTAP object store server manages data as objects, as opposed to other storage architectures such as file or block storage.

To create an object store server using the ONTAP CLI, run the following command:

```
vserver object-store-server create
-vserver <name>
-object-store-server <FQDN>
-certificate-name <name>
-secure-listener-port <443>
-is-http-enabled <false>
```

Create a Bucket

To create a bucket using the ONTAP CLI, run the following command:

```
vserver object-store-server bucket create
-vserver <name>
-bucket <name>
-type nas
-nas-path <junction_path>
```

Caution

- Because S3 in multiprotocol NAS volumes uses pre-existing FlexVol or FlexGroup volumes, a new FlexGroup volume exclusively for S3 objects is not created. The volume already exists, so there is no need to define aggregates, constituent volumes, or size.
- ONTAP S3 supports object versioning in native S3 buckets. Object versioning is not supported in multiprotocol NAS volumes. Consider using SnapMirror instead.

Enable Name Mapping

User authorization is required on all ONTAP object stores to restrict connectivity to authorized clients. When using S3 in multiprotocol NAS volumes, ONTAP must be able to map S3 users to pre-existing users created with Unix or Windows security styles.

To map S3 users to existing Unix and/or Windows users, run the following command:

```
vserver name-mapping create
-vserver <name>
-direction <s3-win|s3-unix>
-position <1|2>
-pattern <S3 user>
-replacement <unix or windows user>
```

Create a Bucket Policy

To set a bucket permission statement using the ONTAP CLI, run the following command:

```
vserver vserver object-store-server bucket policy add-statement
-vserver <data svm>
-bucket <name>
-effect <allow/deny>
-action <*, GetObject, PutObject, DeleteObject, ListBucket, etc.>
-principal <S3 user or group> (maximum of 10 per policy)
-resource <bucket name, bucket-name/*>
```

To view the user's access and secret key by using the ONTAP CLI, run the following command:

Caution

Advanced privilege level is required.

```
object-store-server user show
```

8. Lifecycle Rules

Beginning in ONTAP 9.13.1, ONTAP S3 supports expiration rules that can be used to provide bucket-level information lifecycle management (ILM) capabilities. Using expiration rules, retention policies can be created that apply to specific objects in ONTAP S3 buckets. Each expiration rule consists of:

- Metadata containing the rule ID and status indicating whether the rule is enabled or disabled.
- One or more expiration actions. Options include: Expiration, Noncurrent Version Expiration, and Abort Incomplete Multipart Upload.
- Filters used to match the set of objects that needs to be deleted. Filters include object prefix, tags, object size, age, etc. If no filters are set, the expiration rule will be applied to all objects in the bucket.

After a bucket lifecycle rule has been created, the expiration rule will be added to the header of all new objects put in the bucket.

Caution

ONTAP S3 does not support transition rules.

Expiration

To create a bucket expiration rule using the ONTAP CLI, run the following command:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <name>
-bucket <name>
-rule-id <name>
-index <#>
-is-enabled <true|false>
-action Expiration
-obj-age-days <#>
-obj-exp-date <"MM/DD/YYYY HH:MM:SS">
-expired-obj-del-marker <true|false>
-prefix <name>
-tags <name, name> (maximum of 4)
-obj-size-greater-than <#[KB|MB|GB|TB|PB]>
-obj-size-less-than <#[KB|MB|GB|TB|PB]>
```

Examples

- Expire objects starting with ‘test’ after 30 days

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver svm1
-bucket mybucket
-rule-id rule1
-index 1
-is-enabled true
-action Expiration
-prefix testobj
-obj-age-days 30
```

- Expire objects tagged “proj1=test” on January 1st, 2025

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver svm1
-bucket mybucket
-rule-id rule2
-index 2
-is-enabled true
-action Expiration
-tags proj1=test
-obj-exp-date "2025-01-01T00:00:00"
```

- Expire objects ranging between 100MB and 1GB after 365 days

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver svm1
-bucket mybucket
-rule-id rule3
-index 3
-is-enabled true
-action Expiration
-obj-size-greater-than 100MB
-obj-size-less-than 1GB
-obj-age-days 365
```

Noncurrent Version Expiration

To create a bucket noncurrent version expiration rule using the ONTAP CLI, run the following command:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <name>
-bucket <name>
-rule-id <name>
-index <#>
-is-enabled <true|false>
-action NonCurrentVersionExpiration
-new-non-curr-versions <#>
-non-curr-days <#>
-prefix <name>
-tags <name, name> (maximum of 4)
-obj-size-greater-than <#[KB|MB|GB|TB|PB]
-obj-size-less-than <#[KB|MB|GB|TB|PB]>
```

Examples

- Expire non-current versions of objects after 30 days, retaining up to 10 non-current versions

```
vserver server object-store-server bucket lifecycle-management-rule create
-vserver svm1
-bucket mybucket
-rule-id rule4
-index 4
-action NoncurrentVersionExpiration
-is-enabled true
-non-curr-days 30
-new-non-curr-versions 10
```

Abort Incomplete Multipart Upload

To create a bucket Abort Incomplete Multipart Upload rule using the ONTAP CLI, run the following command:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <name>
-bucket <name>
-rule-id <name>
-index <#>
-is-enabled <true|false>
-action AbortIncompleteMultipartUpload
-after-initiation-days <#>
-prefix <name>
-obj-size-greater-than <#[KB|MB|GB|TB|PB]>
-obj-size-less-than <#[KB|MB|GB|TB|PB]>
```

Examples

- Abort incomplete multipart uploads after 7 days

```
vserver object-store-server bucket lifecycle-management rule create
-vserver svm1
-bucket mybucket
-rule-id rule4
-index 4
-action AbortIncompleteMultipartUpload
-is enabled true
-after-initiation-days 7
```

9. Security

Local Tier

Storage Encryption (SE), Volume Encryption (VE), and Aggregate Encryption (AE) work equally well for objects written to buckets in ONTAP. Neither SE, VE, nor AE are required for S3 in ONTAP.

Over the Wire

TLS/SSL encryption is enabled by default using a system-generated certificate. Using signed certificates from a third-party certificate authority is a recommended best practice.

Client-object store communication without TLS encryption (HTTP, Port 80) is supported but is not a recommended best practice.

Signature Version 4

Prior to ONTAP 9.11.1, S3 in ONTAP did not support Signature Version 2 (v2 signatures) and required the use of v4 signatures.

Caution

Prior to ONTAP 9.11.1, using v2 signatures results in a failure to connect. It is important to be aware of this because many client applications, including commonly used S3 browsers, use v2 signatures by default. Fujitsu recommends that client applications use v4 signatures when possible.

10. S3 SnapMirror

Beginning with ONTAP 9.10.1, data in ONTAP S3 buckets can be protected by S3 SnapMirror. SnapMirror allows you to define synchronization schedules to meet specific recovery point objectives (RPOs). SnapMirror can also be used to create a variety of data protection relationships including source-to-destination, fan-out, and cascading. Fan-in relationships are not supported.

S3 SnapMirror has two primary use cases:

- Backup and recovery, where the objective is to restore from the destination bucket to the source bucket with no intention of failing over to the destination bucket. If the S3 SnapMirror relationship is broken, objects in the destination bucket remain read-only.
- Disaster recovery (DR) and failover, where the objective is to be able to serve data to client applications from the destination bucket in the event a disaster event takes place. If the S3 SnapMirror relationship is broken, the destination bucket supports reads and writes. ONTAP is the only destination target that supports DR and failover operations.

Caution

S3 SnapMirror is exclusively for the protection of native S3 objects. NAS and SAN data tiered by FabricPool to ONTAP S3 buckets is protected as normal using SnapMirror or other data protection applications—not S3 SnapMirror.

Snapshot Copies

Although ONTAP S3 supports object versioning, because object storage is not transactional like file or block storage, S3 SnapMirror does not make use of Snapshot copies that capture the state of a file at a specific point in time and act as highly efficient point-in-time deltas.

Protecting Buckets using S3 SnapMirror

The full set of instructions for mirroring bucket data, setting data protection policies restoring data, and performing takeover operations is found in the related manuals in Fujitsu manual site.

Requirements

S3 SnapMirror requires ONTAP 9.10.1 or later. Prior to ONTAP 9.10.1, data protection could be achieved by using Cloud Sync.

Destination Targets

- Fujitsu
  - ONTAP
  - Cloud Volumes ONTAP for AWS
  - Cloud Volumes ONTAP for Azure
  - Amazon FSx for NetApp ONTAP
  - Cloud Volumes ONTAP of FUJITSU Hybrid IT Service for Microsoft Azure
- Third party
  - Amazon S3

Caution

When using ONTAP as a destination target, S3 SnapMirror supports creating a data protection relationship between source and destination buckets in both same- and remote-cluster relationships. Same-cluster relationships do not protect data from cluster or site-wide disaster events. Fujitsu recommends using S3 SnapMirror with destination targets outside the local cluster.

License

Enabling S3 SnapMirror requires the use of the Data Protection Bundle. Both the Data Protection Bundle and the Hybrid Cloud Bundle are required when using S3 SnapMirror to replicate data to third-party object stores such as Amazon S3.

Certificate Authority (CA) Certification

When using TLS, S3 SnapMirror must be configured to use the destination's CA certificates on both the source and the destination.

Although CA certificates are not required, ONTAP S3 uses TLS and self-signed certificates by default. Using signed certificates from a third-party certificate authority is the recommended best practice.

Cluster Peer Relationship

A cluster peer relationship must be established before using a different ONTAP cluster as an S3 SnapMirror target destination. For more information, see Prepare for mirroring and vaulting and Create a cluster peer relationship.

Cloud Object Store

A cloud object store—such as StorageGRID, Amazon S3, or Microsoft Azure Blob Storage—must be identified by ONTAP before it can be used as a S3 SnapMirror target destination. For more information, see Add a Cloud Object Store.

Protection Policies

S3 SnapMirror creates a data protection relationship that replicates data in a source bucket to a destination bucket. Replication of data is based on the protection policy selected when a bucket is protected. The S3 SnapMirror default protection policy, `Continuous`, replicates data continuously to the destination bucket, using a one-hour RPO, and does not throttle data.

Protection policies can be created and saved for use when protecting one or more buckets. Customizable parameters include the following:

- Policy type
  S3 SnapMirror protection policies must use the Continuous policy type. Asynchronous and Synchronous policies can be created using the Add Protection Policy menu but cannot be selected as a protection policy when protecting a bucket.
- Throttle
  Set the maximum bandwidth allowed to attain the RPO. The default of zero does not set any throttle.
- RPO
  Set a delay between the time a change is made in the source bucket and when that change is pushed to the destination bucket. The default is one hour.

11. Supported S3 Actions

Buckets

Actions marked with an asterisk are supported by ONTAP but not by S3 REST APIs.

- CreateBucket (9.11.1)
- DeleteBucket (9.11.1)
- DeleteBucketLifecycleConfiguration (9.13.1)
- DeleteBucketPolicy (9.12.1)
- GetBucketAcl
- GetBucketLifecycleConfiguration (9.13.1)
- GetBucketLocation (9.10.1)
- GetBucketPolicy (9.12.1)
- GetBucketVersioning (9.11.1)
- HeadBucket
- ListBuckets
- ListBucketVersioning (9.11.1)
- PutBucket*
- PutBucketLifecycleConfiguration (9.13.1)
- PutBucketPolicy (9.12.1)
- PutBucketVersioning (9.11.1)

Objects

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject (9.12.1)
- CreateMultipartUpload
- DeleteObject
- DeleteObjects (9.11.1)
- DeleteObjectTagging (9.9.1)
- GetObject
- GetObjectAcl
- GetObjectTagging (9.9.1)
- HeadObject
- ListMultipartUpload
- ListObjectVersions (9.11.1)
- ListObjects
- ListParts
- PutObject
- PutObjectTagging (9.9.1)
- HeadObject
- UploadPart
- UploadPartCopy (9.12.1)

Group Policies

These operations are not specific to S3 and are generally associated with Identity and Management (IAM). ONTAP supports these commands but does not use the IAM REST APIs.

ONTAP S3 groups can have a maximum of 10 attached policies. Group policies can have a maximum of five statements. Each statement can have a maximum of 10 resources.

- Create Policy
- AttachGroup Policy

User Management

These operations are not specific to S3 and are generally associated with IAM:

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

Not Supported in Multiprotocol NAS Volumes

Actions and capabilities associated with metadata, multipart objects, tags, and versioning are not supported when using S3 in multiprotocol NAS volumes. This includes the following:

- Key-values pairs using `x-amz-meta-<key>` are not saved, and request headers using `x-amz-meta` are ignored.
- Requests to update tags are rejected, and headers using `x-amz-tagging` are ignored.
- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- DeleteObjectTagging
- GetBucketVersioning
- GetObjectTagging
- PutBucketVersioning
- PutObjectTagging
- ListBucketVersioning
- ListMultipartUpload
- ListObjectVersions

12. S3 Actions by Release

ONTAP 9.13.1

ONTAP 9.13.1 adds bucket lifecycle configuration.

- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

ONTAP 9.12.1

ONTAP 9.12.1 adds bucket policies and the ability to copy objects.

- DeleteBucketPolicy
- GetBucketPolicy
- PutBucketPolicy
- CopyObject
- UploadPartCopy

ONTAP 9.11.1

ONTAP 9.11.1 adds versioning, presigned URLs, chunked uploads, and support for common S3 actions such as creating and deleting buckets using S3 APIs.

- ONTAP S3 now supports chunked uploads signing requests using `x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD`
- ONTAP S3 now supports client applications using presigned URLs to share objects or allow other users to upload objects without requiring user credentials.
- CreateBucket
- DeleteBucket
- GetBucketVersioning
- ListBucketVersioning
- PutBucketVersioning
- DeleteObjects
- ListObjectVersions

Caution

Because the underlying FlexGroup is not created until the first bucket is, a bucket must first be created in ONTAP before an external client can create a bucket using CreateBucket.

ONTAP 9.10.1

ONTAP 9.10.1 adds support for S3 SnapMirror and GetBucketLocation.

- GetBucketLocation

ONTAP 9.9.1

ONTAP 9.9.1 adds object metadata and tagging support to ONTAP S3.

- PutObject and CreateMultipartUpload now include key-value pairs using `x-amz-meta-<key>`. For example: `x-amz-meta-project: ontap_s3`.
- GetObject and HeadObject now return user-defined metadata.
- Tags can also be used with buckets. Unlike metadata, tags can be read independently of objects using:
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging

13. Interoperability

The exceptions to normal interoperability listed in Table 1 are unique to ONTAP object stores.

Table 1 S3 interoperability

Focus	Supported	Not supported
Data protection	• Cloud Sync • S3 SnapMirror (9.10.1) • Unmirrored MetroCluster aggregates (9.12.1)	• Erasure coding • Mirrored MetroCluster aggregates • NDMP • SnapLock technology • SnapMirror technology • SyncMirror technology • SMTape • SVM-DR • WORM
Encryption	• Aggregate Encryption (AE) • Storage Encryption (SE) • Volume Encryption (VE) • TLS/SSL	• SLAG
Storage efficiency	• Compression • Compaction • Deduplication • Temperature Sensitive Storage Efficiency (TSSE)	Aggregate-level efficiencies
Storage virtualization	–	FlexArray technology
QoS	• QoS maximums (ceiling) • QoS minimums (floors)	–
Additional features	• Audit • Bucket Lifecycle Management (9.13.1) • FabricPool cloud tier (native S3 only) • FabricPool local tier (NAS volumes only)	• FabricPool cloud tier (NAS volumes only) • FabricPool local tier (native S3 only) • FPolicy software • Qtrees • Quotas

Fujitsu Storage
ETERNUS AX series All-Flash Arrays,
ETERNUS HX series Hybrid Arrays
S3 in ONTAP Best Practices
ONTAP 9.13.1

P3AG-6642-02ENZ0

Date of issuance: November 2023
Issuance responsibility: Fujitsu Limited

- The content of this manual is subject to change without notice.
- This manual was prepared with the utmost attention to detail.
  However, Fujitsu shall assume no responsibility for any operational problems as the result of errors, omissions, or the use of information in this manual.
- Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
- The content of this manual may not be reproduced or distributed in part or in its entirety without prior permission from Fujitsu.

FUJITSU