S3 support in ONTAP 9

ONTAP 9

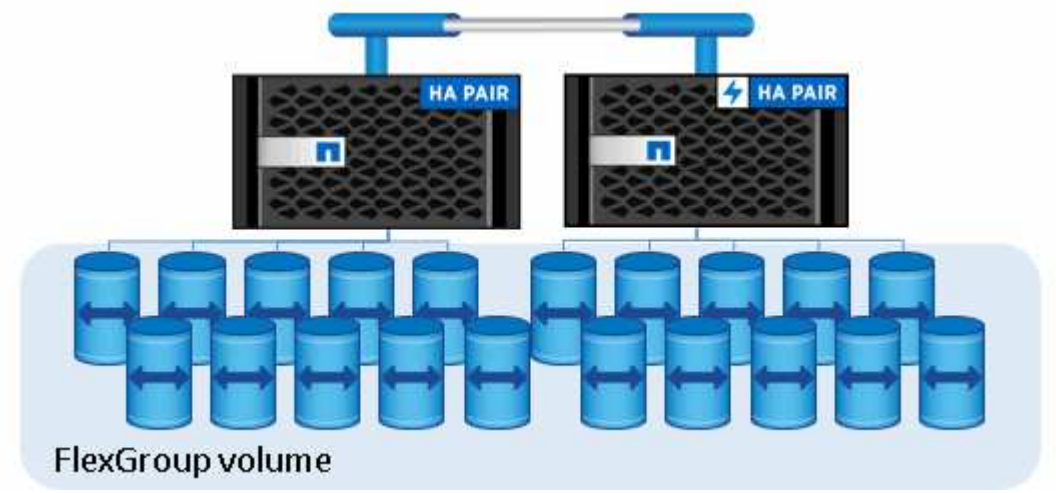
NetApp
February 10, 2022

Table of Contents

S3 support in ONTAP 9

ONTAP S3 architecture and use cases

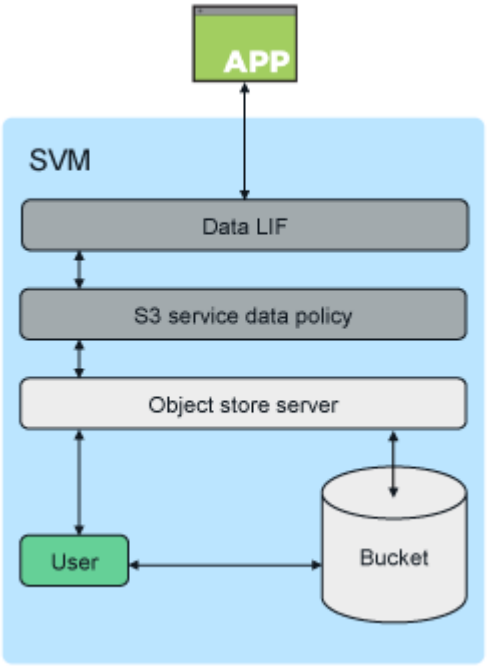
In ONTAP, the underlying architecture for a bucket is a FlexGroup volume—a single namespace that is made up of multiple constituent member volumes but is managed as a single volume.



Buckets are only limited by the physical maximums of the underlying hardware, architectural maximums could be higher. Buckets can take advantage of FlexGroup elastic sizing to automatically grow a constituent of a FlexGroup volume if it is running out of space. There is a limit of 1000 buckets per FlexGroup volume, or 1/3 of the FlexGroup volume's capacity (to account for data growth in buckets).

No NAS or SAN protocol access is permitted to the FlexGroup volume that contain S3 buckets.

Access to the bucket is provided through authorized users and client applications.



There are three primary use cases for client access to ONTAP S3 services:

- For ONTAP systems using ONTAP S3 as a remote FabricPool capacity (cloud) tier

  The S3 server and bucket containing the capacity tier (for *cold* data) is on a different cluster than the performance tier (for *hot* data).

- For ONTAP systems using ONTAP S3 as a local FabricPool tier

  The S3 server and bucket containing the capacity tier is on the same cluster, but on a different HA pair, as the performance tier.

- For external S3 client apps

  ONTAP S3 serves S3 client apps run on non-NetApp systems.

It is a best practice to provide access to ONTAP S3 buckets using HTTPS. When HTTPS is enabled, security certificates are required for proper integration with SSL/TLS. Client users' access and secret keys are then required to authenticate the user with ONTAP S3 as well as authorizing the users' access permissions for operations within ONTAP S3. The client application should also have access to the root CA certificate (the ONTAP S3 server's signed certificate) to be able to authenticate the server and create a secure connection between client and server.

Users are created within the S3-enabled SVM, and their access permissions can be controlled at the bucket or SVM level; that is, they can be granted access to one or more buckets within the SVM.

HTTPS is enabled by default on ONTAP S3 servers. It is possible to disable HTTPS and enable HTTP for client access, in which case authentication using CA certificates is not required. However, when HTTP is enabled and HTTPS is disabled, all communication with the ONTAP S3 server are sent over the network in clear text.

For additional information, see Technical Report: S3 in ONTAP Best Practices

Related information

FlexGroup volumes management

ONTAP version support for S3 object storage

In ONTAP 9.7, S3 object storage was introduced as a public preview. That version was not intended for production environments and will no longer be updated as of ONTAP 9.8. Only ONTAP 9.8 and later releases support S3 object storage in production environments.

S3 buckets created with the 9.7 public preview can be used in ONTAP 9.8 and later, but cannot take advantage of feature enhancements. If you have buckets created with the 9.7 public preview, you should migrate the contents of those buckets to 9.8 buckets for feature support, security, and performance enhancements.

In ONTAP 9.9.1 and later releases, ONTAP S3 is supported with Cloud Volumes ONTAP for Azure, but not for AWS or Google Cloud.

ONTAP S3 supported actions

Bucket operations

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

- DeleteBucket*
- DeleteBucketPolicy*
- GetBucketAcl
- HeadBucket
- ListBuckets
- PutBucket*

Object operations

Beginning with ONTAP 9.9.1, ONTAP S3 supports object metadata and tagging.

- 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.
- Unlike metadata, tags can be read independently of objects using:
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging

Supported object actions:

- PutObject
- PutObjectTagging (beginning with ONTAP 9.9.1)
- GetObject
- GetObjectAcl
- GetObjectTagging (beginning with ONTAP 9.9.1)
- DeleteObject
- DeleteObjectTagging (beginning with ONTAP 9.9.1)
- HeadObject
- ListObjects
- ListObjectsV2
- ListParts
- UploadPart
- AbortMultipartUpload
- CompleteMultipartUpload

- CreateMultipartUpload
- ListMultipartUpload

Group policies

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

- Create Policy
- AttachGroup Policy

User management

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

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

ONTAP S3 interoperability

The ONTAP S3 server interacts normally with other ONTAP functionality except as noted in this table.

Feature area	Supported	Not supported
Cloud Volumes ONTAP	Azure clients in ONTAP 9.9.1 and later releases	Cloud Volumes ONTAP for any client in ONTAP 9.8 and earlier releases

Feature area	Supported	Not supported
Data protection	• Cloud Sync	• Erasure coding • Information lifecycle management • MetroCluster • NDMP • Object versioning • SMTape • SnapLock • SnapMirror • SnapMirror Cloud • SVM disaster recovery • SyncMirror • User-created Snapshot copies • WORM
Encryption	• NetApp Aggregate Encryption (NAE) • NetApp Volume Encryption (NVE) • NetApp Storage Encryption (NSE) • TLS/SSL	• SLAG
Storage efficiency	• Deduplication • Compression • Compaction	• Aggregate-level efficiencies • Volume clone of the FlexGroup volume containing ONTAP S3 buckets
Storage virtualization	-	NetApp FlexArray Virtualization
Quality of service (QoS)	• QoS maximums (ceilings) • QoS minimums (floors)	-
Additional features	-	• Audit • FlexCache volumes • FPolicy • Qtrees • Quotas