S3 support in ONTAP 9

ONTAP 9

NetApp
August 04, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/s3-config/s3-support-concept.html on August 04, 2022. Always check docs.netapp.com for the latest.

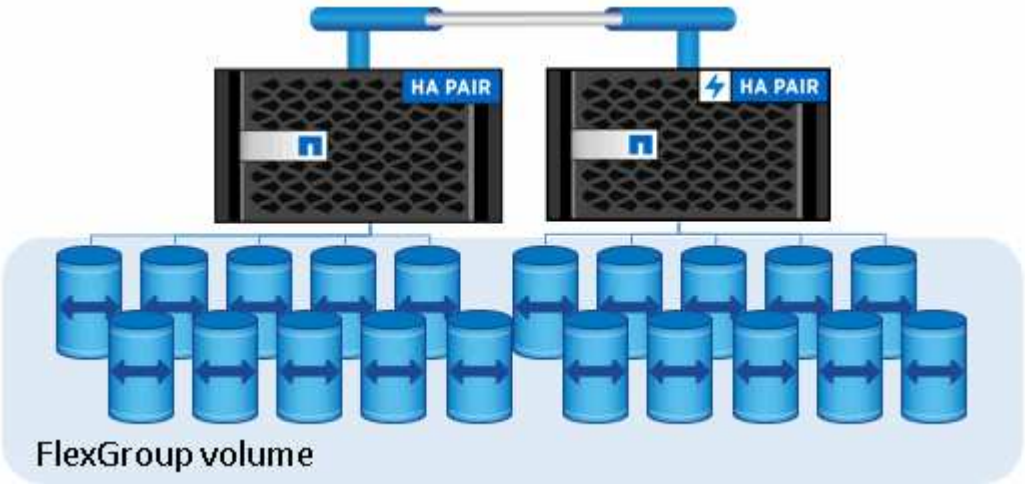
Table of Contents

S3 support in ONTAP 9 . . . 1
ONTAP S3 architecture and use cases . . . 1
ONTAP version support for S3 object storage . . . 2
ONTAP S3 supported actions . . . 3
ONTAP S3 interoperability . . . 5

S3 support in ONTAP 9

ONTAP S3 architecture and use cases

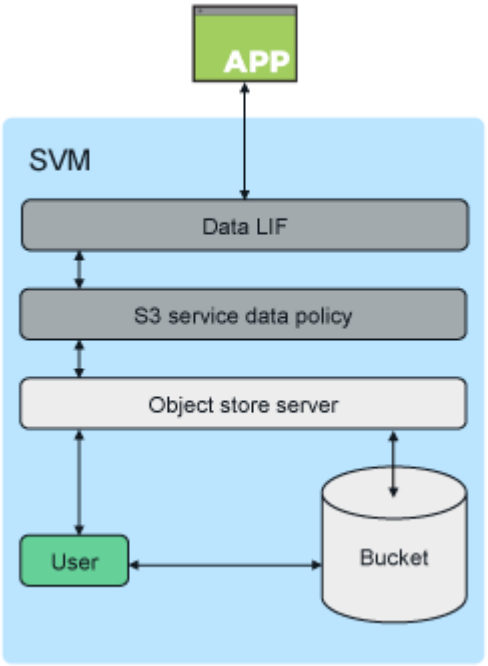
In ONTAP, the underlying architecture for a bucket is a FlexGroup volume—a single namespace that is made up of multiple constituent member volumes but is managed as a single volume.



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

ONTAP supports S3 object storage for on-premises environments beginning with ONTAP 9.8. Cloud Volumes ONTAP supports S3 object storage for cloud environments beginning with ONTAP 9.9.1.

S3 support with Cloud Volumes ONTAP

ONTAP S3 is configured and functions the same in Cloud Volumes ONTAP as in on-premises environments, with one exception:

- Underlying aggregates should be from one node only. Learn more about bucket creation in CVO environments.

Cloud Provider	ONTAP Version
Azure	ONTAP 9.9.1 and later

Cloud Provider	ONTAP Version
AWS	ONTAP 9.11.0 and later
Google Cloud	Not currently supported

S3 public preview in ONTAP 9.7

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.

ONTAP S3 supported actions

Bucket operations

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

- CreateBucket (beginning with ONTAP 9.11.1)
- DeleteBucket* (supported with S3 REST APIs beginning with ONTAP 9.11.1)
- 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

Beginning with ONTAP 9.11.1, ONTAP S3 supports object versioning and associated actions with these ONTAP APIs:

- PutBucketVersioning

- GetBucketVersioning
- ListBucketVersions

Supported object actions:

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- DeleteObject
- DeleteObjects (supported with S3 REST APIs beginning with ONTAP 9.11.1)
- DeleteObjectTagging (beginning with ONTAP 9.9.1)
- GetBucketVersioning (beginning with ONTAP 9.11.1)
- GetObject
- GetObjectAcl
- GetObjectTagging (beginning with ONTAP 9.9.1)
- HeadObject
- ListMultipartUpload
- ListObjects
- ListObjectsV2
- ListBucketVersions (beginning with ONTAP 9.11.1)
- ListParts
- PutBucketVersioning (beginning with ONTAP 9.11.1)
- PutObject
- PutObjectTagging (beginning with ONTAP 9.9.1)
- UploadPart

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 • AWS clients in ONTAP 9.11.0 and later releases	• Cloud Volumes ONTAP for any client in ONTAP 9.8 and earlier releases • Google Cloud clients
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

Feature area	Supported	Not supported
Quality of service (QoS)	• QoS maximums (ceilings) • QoS minimums (floors)	-
Additional features	-	• Audit • FlexCache volumes • FPolicy • Qtrees • Quotas

Copyright Information

Copyright © 2022 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.