



Storage

Cloud Volumes ONTAP

NetApp
September 28, 2022

This PDF was generated from <https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/aws/concept-client-protocols.html> on September 28, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- Storage 1
 - Client protocols 1
 - Disks and aggregates 1
 - Elastic Volumes in AWS 3
 - Data tiering overview 9
 - Storage management 11
 - Write speed 14
 - Flash Cache 16
 - WORM storage 17

Storage

Client protocols

Cloud Volumes ONTAP supports the iSCSI, NFS, SMB, and S3 client protocols.

iSCSI

iSCSI is a block protocol that can run on standard Ethernet networks. Most client operating systems offer a software initiator that runs over a standard Ethernet port.

NFS

NFS is the traditional file access protocol for UNIX and LINUX systems. Clients can access files in ONTAP volumes using the NFSv3, NFSv4, and NFSv4.1 protocols. You can control file access using UNIX-style permissions, NTFS-style permissions, or a mix of both.

Clients can access the same files using both NFS and SMB protocols.

SMB

SMB is the traditional file access protocol for Windows systems. Clients can access files in ONTAP volumes using the SMB 2.0, SMB 2.1, SMB 3.0, and SMB 3.1.1 protocols. Just like with NFS, a mix of permission styles are supported.

S3

Cloud Volumes ONTAP supports S3 as an option for scale-out storage in the following cloud providers:

- AWS

S3 protocol support enables you to configure S3 client access to objects contained in a bucket in an SVM.

[Learn how to configure and manage S3 object storage services in ONTAP.](#)

Disks and aggregates

Understanding how Cloud Volumes ONTAP uses cloud storage can help you understand your storage costs.



All disks and aggregates must be created and deleted directly from Cloud Manager. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

Overview

Cloud Volumes ONTAP uses cloud provider storage as disks and groups them into one or more aggregates. Aggregates provide storage to one or more volumes.



Several types of cloud disks are supported. You choose the disk type when you create a volume and the default disk size when you deploy Cloud Volumes ONTAP.



The total amount of storage purchased from a cloud provider is the *raw capacity*. The *usable capacity* is less because approximately 12 to 14 percent is overhead that is reserved for Cloud Volumes ONTAP use. For example, if Cloud Manager creates a 500 GiB aggregate, the usable capacity is 442.94 GiB.

AWS storage

In AWS, Cloud Volumes ONTAP uses EBS storage for user data and local NVMe storage as Flash Cache on some EC2 instance types.

EBS storage

In AWS, an aggregate can contain up to 6 disks that are all the same size. But if you have a configuration that supports the Amazon EBS Elastic Volumes feature, then an aggregate can contain up to 8 disks. [Learn more about support for Elastic Volumes.](#)

The maximum disk size is 16 TiB.

The underlying EBS disk type can be either General Purpose SSDs (gp3 or gp2), Provisioned IOPS SSD (io1), or Throughput Optimized HDD (st1). You can pair an EBS disk with Amazon S3 to [tier inactive data to low-cost object storage](#).



Tiering data to object storage is not recommended when using Throughput Optimized HDDs (st1).

Local NVMe storage

Some EC2 instance types include local NVMe storage, which Cloud Volumes ONTAP uses as [Flash Cache](#).

Related links

- [AWS documentation: EBS Volume Types](#)
- [Learn how to choose disk types and disk sizes for your systems in AWS](#)
- [Review storage limits for Cloud Volumes ONTAP in AWS](#)
- [Review supported configurations for Cloud Volumes ONTAP in AWS](#)

RAID type

The RAID type for each Cloud Volumes ONTAP aggregate is RAID0 (striping). Cloud Volumes ONTAP relies on the cloud provider for disk availability and durability. No other RAID types are supported.

Hot spares

RAID0 doesn't support the use of hot spares for redundancy.

Creating unused disks (hot spares) attached to a Cloud Volumes ONTAP instance is an unnecessary expense and may prevent provisioning additional space as needed. Therefore, it's not recommended.

Elastic Volumes in AWS

Support for the Amazon EBS Elastic Volumes feature with a Cloud Volumes ONTAP aggregate provides better performance and additional capacity, while enabling Cloud Manager to automatically increase the underlying disk capacity as needed.

Benefits

- Dynamic disk growth

Cloud Manager can dynamically increase the size of disks while Cloud Volumes ONTAP is running and while disks are still attached.

- Better performance

Aggregates that are enabled with Elastic Volumes can have up to eight disks that are equally utilized across two RAID groups. This configuration provides more throughput and consistent performance.

- Larger aggregates

Support for eight disks provides a maximum aggregate capacity of 128 TiB. These limits are higher than the six disk limit and 96 TiB limit for aggregates that aren't enabled with the Elastic Volumes feature.

Note that total system capacity limits remain the same.

[Learn more about Elastic Volumes from AWS](#)

Supported configurations

The Amazon EBS Elastic Volumes feature is supported with specific Cloud Volumes ONTAP versions and specific EBS disk types.

Cloud Volumes ONTAP version

The Elastic Volumes feature is supported with *new* Cloud Volumes ONTAP systems created from version 9.11.0 or later. The feature is *not* supported with existing Cloud Volumes ONTAP systems that were deployed prior to 9.11.0.

For example, the Elastic Volumes feature is not supported if you created a Cloud Volumes ONTAP 9.9.0 system and then later upgraded that system to version 9.11.0. It must be a new system deployed using version 9.11.0 or later.

EBS disk types

The Elastic Volumes feature is automatically enabled at the aggregate level when using General Purpose SSDs (gp3) or Provisioned IOPS SSDs (io1). The Elastic Volumes feature is not supported with aggregates that use any other disk type.

Required AWS permissions

Starting with the 3.9.19 release, the Connector requires the following permissions to enable and manage the Elastic Volumes feature on a Cloud Volumes ONTAP aggregate:

- ec2:DescribeVolumesModifications
- ec2:ModifyVolume

These permissions are included in [the policies provided by NetApp](#)

How support for Elastic Volumes works

An aggregate that has the Elastic Volumes feature enabled is comprised of one or two RAID groups. Each RAID group has four identical disks that have the same capacity. Here's an example of a 10 TiB aggregate that has four disks that are 2.5 TiB each:



When Cloud Manager creates an aggregate, it starts with one RAID group. If additional capacity is needed, Cloud Manager grows the aggregate by increasing the capacity of all disks in the RAID group by the same amount. The capacity increase is either a minimum of 256 GiB or 10% of the aggregate's size.

For example, if you have a 1 TiB aggregate, each disk is 250 GiB. 10% of the aggregate's capacity is 100 GiB. That's lower than 256 GiB, so the size of the aggregate is increased by the 256 GiB minimum (or 64 GiB for each disk).

Cloud Manager increases the size of the disks while the Cloud Volumes ONTAP system is running and while the disks are still attached. The change is non-disruptive.

If an aggregate reaches 64 TiB (or 16 TiB on each disk), Cloud Manager creates a second RAID group for additional capacity. This second RAID group works just like the first one: it has four disks that have the exact same capacity and it can grow up to 64 TiB. That means an aggregate can have a maximum capacity of 128 TiB.

Here's an example of an aggregate with two RAID groups. The capacity limit has been reached on the first RAID group, while the disks in the second RAID group have plenty of free space.



What happens when you create a volume

If you create a volume that uses gp3 or io1 disks, Cloud Manager creates the volume on an aggregate as follows:

- If there is an existing gp3 or io1 aggregate that has Elastic Volumes enabled, Cloud Manager creates the volume on that aggregate.

- If there are multiple gp3 or io1 aggregates that have Elastic Volumes enabled, Cloud Manager creates the volume on the aggregate that requires the least amount of resources.
- If the system only has gp3 or io1 aggregates that aren't enabled for Elastic Volumes, then the volume is created on that aggregate.



While this scenario is unlikely, it's possible in two cases:

- You explicitly disabled the Elastic Volumes feature when creating an aggregate from the API.
- You created a new Cloud Volumes ONTAP system from the user interface, in which case the Elastic Volumes feature is disabled on the initial aggregate. Review [Limitations](#) below to learn more.

- If no existing aggregates have enough capacity, Cloud Manager creates the aggregate with Elastic Volumes enabled and then creates the volume on that new aggregate.

The size of the aggregate is based on the requested volume size plus an additional 10% capacity.

Capacity Management Mode

The Capacity Management Mode for a Connector works with Elastic Volumes similar to how it works with other types of aggregates:

- When Automatic mode is enabled (this is the default setting), Cloud Manager automatically increases the size of aggregates if additional capacity is needed.
- If you change the capacity management mode to Manual, Cloud Manager asks for your approval to purchase additional capacity.

[Learn more about the Capacity Management Mode.](#)

Limitations

Increasing the size of an aggregate can take up to 6 hours. During that time, Cloud Manager can't request any additional capacity for that aggregate.

How to work with Elastic Volumes

You can work with Elastic Volumes in Cloud Manager as follows:

- Create a new system that has Elastic Volumes enabled on the initial aggregate when using gp3 or io1 disks

[Learn how to create Cloud Volumes ONTAP system](#)

- Create a new volume on an aggregate that has Elastic Volumes enabled

If you create a volume that uses gp3 or io1 disks, Cloud Manager automatically creates the volume on an aggregate that has Elastic Volumes enabled. For more details, refer to [What happens when you create a volume.](#)

[Learn how to create volumes.](#)

- Create a new aggregate that has Elastic Volumes enabled

Elastic Volumes is automatically enabled on new aggregates that use gp3 or io1 disks, as long as the Cloud Volumes ONTAP system was created from version 9.11.0 or later.

When you create the aggregate, Cloud Manager will prompt you for the aggregate's capacity size. This is different than other configurations where you choose a disk size and number of disks.

The following screenshot shows an example of a new aggregate comprised of gp3 disks.

[Learn how to create aggregates.](#)

- Identify aggregates that have Elastic Volumes enabled

When you go to the Advanced Allocation page, you can identify whether the Elastic Volumes feature is enabled on an aggregate. In the following example, aggr2 has Elastic Volumes enabled whereas aggr1 does not.

- Add capacity to an aggregate

While Cloud Manager automatically adds capacity to aggregates as needed, you can manually increase the capacity yourself.

[Learn how to increase aggregate capacity.](#)

- Replicate data to an aggregate that has Elastic Volumes enabled

If the destination Cloud Volumes ONTAP system supports Elastic Volumes, a destination volume will be placed on an aggregate that has Elastic Volumes enabled (as long as you choose a gp3 or io1 disk).

[Learn how to set up data replication](#)

Data tiering overview

Reduce your storage costs by enabling automated tiering of inactive data to low-cost object storage. Active data remains in high-performance SSDs or HDDs, while inactive data is tiered to low-cost object storage. This enables you to reclaim space on your primary storage and shrink secondary storage.



Data tiering is powered by FabricPool technology.



You don't need to install a feature license to enable data tiering (FabricPool).

Data tiering in AWS

When you enable data tiering in AWS, Cloud Volumes ONTAP uses EBS as a performance tier for hot data and AWS S3 as a capacity tier for inactive data.

Performance tier

The performance tier can be General Purpose SSDs (gp3 or gp2) or Provisioned IOPS SSDs (io1).

Tiering data to object storage is not recommended when using Throughput Optimized HDDs (st1).

Capacity tier

A Cloud Volumes ONTAP system tiers inactive data to a single S3 bucket.

Cloud Manager creates a single S3 bucket for each working environment and names it *fabric-pool-cluster unique identifier*. A different S3 bucket is not created for each volume.

When Cloud Manager creates the S3 bucket, it uses the following default settings:

- Storage class: Standard
- Default encryption: Disabled
- Block public access: Block all public access
- Object ownership: ACLs enabled
- Bucket versioning: Disabled
- Object lock: Disabled

Storage classes

The default storage class for tiered data in AWS is *Standard*. Standard is ideal for frequently accessed data stored across multiple Availability Zones.

If you don't plan to access the inactive data, you can reduce your storage costs by changing the storage class to one of the following: *Intelligent Tiering*, *One-Zone Infrequent Access*, *Standard-Infrequent Access*, or *S3 Glacier Instant Retrieval*. When you change the storage class, inactive data starts in the Standard storage class and transitions to the storage class that you selected, if the data is not accessed after 30 days.

The access costs are higher if you do access the data, so take that into consideration before you change the storage class. [Learn more about Amazon S3 storage classes](#).

You can select a storage class when you create the working environment and you can change it any time after. For details about changing the storage class, see [Tiering inactive data to low-cost object storage](#).

The storage class for data tiering is system wide—it's not per volume.

Data tiering and capacity limits

If you enable data tiering, a system's capacity limit stays the same. The limit is spread across the performance tier and the capacity tier.

Volume tiering policies

To enable data tiering, you must select a volume tiering policy when you create, modify, or replicate a volume. You can select a different policy for each volume.

Some tiering policies have an associated minimum cooling period, which sets the time that user data in a volume must remain inactive for the data to be considered "cold" and moved to the capacity tier. The cooling period starts when data is written to the aggregate.



You can change the minimum cooling period and default aggregate threshold of 50% (more on that below). [Learn how to change the cooling period](#) and [learn how to change the threshold](#).

Cloud Manager enables you to choose from the following volume tiering policies when you create or modify a volume:

Snapshot Only

After an aggregate has reached 50% capacity, Cloud Volumes ONTAP tiers cold user data of Snapshot copies that are not associated with the active file system to the capacity tier. The cooling period is approximately 2 days.

If read, cold data blocks on the capacity tier become hot and are moved to the performance tier.

All

All data (not including metadata) is immediately marked as cold and tiered to object storage as soon as possible. There is no need to wait 48 hours for new blocks in a volume to become cold. Note that blocks located in the volume prior to the All policy being set require 48 hours to become cold.

If read, cold data blocks on the cloud tier stay cold and are not written back to the performance tier. This policy is available starting with ONTAP 9.6.

Auto

After an aggregate has reached 50% capacity, Cloud Volumes ONTAP tiers cold data blocks in a volume to a capacity tier. The cold data includes not just Snapshot copies but also cold user data from the active file system. The cooling period is approximately 31 days.

This policy is supported starting with Cloud Volumes ONTAP 9.4.

If read by random reads, the cold data blocks in the capacity tier become hot and move to the performance tier. If read by sequential reads, such as those associated with index and antivirus scans, the cold data blocks stay cold and do not move to the performance tier.

None

Keeps data of a volume in the performance tier, preventing it from being moved to the capacity tier.

When you replicate a volume, you can choose whether to tier the data to object storage. If you do, Cloud Manager applies the **Backup** policy to the data protection volume. Starting with Cloud Volumes ONTAP 9.6, the **All** tiering policy replaces the backup policy.

Turning off Cloud Volumes ONTAP impacts the cooling period

Data blocks are cooled by cooling scans. During this process, blocks that haven't been used have their block temperature moved (cooled) to the next lower value. The default cooling time depends on the volume tiering policy:

- Auto: 31 days
- Snapshot Only: 2 days

Cloud Volumes ONTAP must be running for the cooling scan to work. If Cloud Volumes ONTAP is turned off, cooling will stop, as well. As a result, you can experience longer cooling times.



When Cloud Volumes ONTAP is turned off, the temperature of each block is preserved until you restart the system. For example, if the temperature of a block is 5 when you turn the system off, the temp is still 5 when you turn the system back on.

Setting up data tiering

For instructions and a list of supported configurations, see [Tiering inactive data to low-cost object storage](#).

Storage management

Cloud Manager provides simplified and advanced management of Cloud Volumes ONTAP storage.



All disks and aggregates must be created and deleted directly from Cloud Manager. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

Storage provisioning

Cloud Manager makes storage provisioning for Cloud Volumes ONTAP easy by purchasing disks and managing aggregates for you. You simply need to create volumes. You can use an advanced allocation option to provision aggregates yourself, if desired.

Simplified provisioning

Aggregates provide cloud storage to volumes. Cloud Manager creates aggregates for you when you launch an instance, and when you provision additional volumes.

When you create a volume, Cloud Manager does one of three things:

- It places the volume on an existing aggregate that has sufficient free space.
- It places the volume on an existing aggregate by purchasing more disks for that aggregate.

In the case of an aggregate in AWS that supports Elastic Volumes, Cloud Manager also increases the size of the disks in a RAID group. [Learn more about support for Elastic Volumes.](#)

- It purchases disks for a new aggregate and places the volume on that aggregate.

Cloud Manager determines where to place a new volume by looking at several factors: an aggregate's maximum size, whether thin provisioning is enabled, and free space thresholds for aggregates.



The Account Admin can modify free space thresholds from the **Settings** page.

Disk size selection for aggregates in AWS

When Cloud Manager creates new aggregates for Cloud Volumes ONTAP in AWS, it gradually increases the disk size in an aggregate, as the number of aggregates in the system increases. Cloud Manager does this to ensure that you can utilize the system's maximum capacity before it reaches the maximum number of data disks allowed by AWS.

For example, Cloud Manager might choose the following disk sizes:

Aggregate number	Disk size	Max aggregate capacity
1	500 GiB	3 TiB
4	1 TiB	6 TiB
6	2 TiB	12 TiB



This behavior does not apply to aggregates that support the Amazon EBS Elastic Volumes feature. Aggregates that have Elastic Volumes enabled are comprised of one or two RAID groups. Each RAID group has four identical disks that have the same capacity. [Learn more about support for Elastic Volumes.](#)

You can choose the disk size yourself by using the advanced allocation option.

Advanced allocation

Rather than let Cloud Manager manage aggregates for you, you can do it yourself. [From the Advanced allocation page](#), you can create new aggregates that include a specific number of disks, add disks to an existing aggregate, and create volumes in specific aggregates.

Capacity management

The Account Admin can choose whether Cloud Manager notifies you of storage capacity decisions or whether Cloud Manager automatically manages capacity requirements for you.

This behavior is determined by the *Capacity Management Mode* on a Connector. The Capacity Management Mode affects all Cloud Volumes ONTAP systems managed by that Connector. If you have another Connector, it can be configured differently.

Automatic capacity management

The Capacity Management Mode is set to automatic by default. In this mode, Cloud Manager automatically purchases new disks for Cloud Volumes ONTAP instances when more capacity is needed, deletes unused collections of disks (aggregates), moves volumes between aggregates when needed, and attempts to unfail disks.

The following examples illustrate how this mode works:

- If an aggregate reaches the capacity threshold and it has room for more disks, Cloud Manager automatically purchases new disks for that aggregate so volumes can continue to grow.

Cloud Manager checks the free space ratio every 15 minutes to determine if it needs to purchase additional disks.

In the case of an aggregate in AWS that supports Elastic Volumes, Cloud Manager also increases the size of the disks in a RAID group. [Learn more about support for Elastic Volumes](#).

- If an aggregate reaches the capacity threshold and it can't support any additional disks, Cloud Manager automatically moves a volume from that aggregate to an aggregate with available capacity or to a new aggregate.

If Cloud Manager creates a new aggregate for the volume, it chooses a disk size that accommodates the size of that volume.

Note that free space is now available on the original aggregate. Existing volumes or new volumes can use that space. The space can't be returned to the cloud provider in this scenario.

- If an aggregate contains no volumes for more than 12 hours, Cloud Manager deletes it.

Management of LUNs with automatic capacity management

Cloud Manager's automatic capacity management doesn't apply to LUNs. When Cloud Manager creates a LUN, it disables the autogrow feature.

Manual capacity management

If the Account Admin set the Capacity Management Mode to manual, Cloud Manager displays Action Required messages when capacity decisions must be made. The same examples described in the automatic mode apply to the manual mode, but it is up to you to accept the actions.

Learn more

[Learn how to modify the capacity management mode.](#)

Write speed

Cloud Manager enables you to choose normal or high write speed for most Cloud Volumes ONTAP configurations. Before you choose a write speed, you should understand the differences between the normal and high settings and risks and recommendations when using high write speed.

Normal write speed

When you choose normal write speed, data is written directly to disk. When data is written directly to disk, reduces the likelihood of data loss in the event of an unplanned system outage, or a cascading failure involving an unplanned system outage (HA pairs only).

Normal write speed is the default option.

High write speed

When you choose high write speed, data is buffered in memory before it is written to disk, which provides faster write performance. Due to this caching, there is the potential for data loss if an unplanned system outage occurs.

The amount of data that can be lost in the event of an unplanned system outage is the span of the last two consistency points. A consistency point is the act of writing buffered data to disk. A consistency point occurs when the write log is full or after 10 seconds (whichever comes first). However, the performance of the storage provided by your cloud provider can affect consistency point processing time.

When to use high write speed

High write speed is a good choice if fast write performance is required for your workload and you can withstand the risk of data loss in the event of an unplanned system outage, or a cascading failure involving an unplanned system outage (HA pairs only).

Recommendations when using high write speed

If you enable high write speed, you should ensure write protection at the application layer, or that the applications can tolerate data loss, if it occurs.

High write speed with an HA pair in AWS

If you plan to enable high write speed on an HA pair in AWS, you should understand the difference in protection levels between a multiple Availability Zone (AZ) deployment and a single AZ deployment. Deploying an HA pair across multiple AZs provides more resiliency and can help to mitigate the chance of data loss.

[Learn more about HA pairs in AWS.](#)

Configurations that support high write speed

Not all Cloud Volumes ONTAP configurations support high write speed. Those configurations use normal write speed by default.

AWS

If you use a single node system, Cloud Volumes ONTAP supports high write speed with all instance types.

Starting with the 9.8 release, Cloud Volumes ONTAP supports high write speed with HA pairs when using almost all supported EC2 instance types, except for m5.xlarge and r5.xlarge.

[Learn more about the Amazon EC2 instances that Cloud Volumes ONTAP supports.](#)

How to select a write speed

You can choose a write speed when you create a new working environment and you can [change the write speed for an existing system](#).

What to expect if data loss occurs

If data loss occurs due to high write speed, the Event Management System (EMS) reports the following two events:

- Cloud Volumes ONTAP 9.11.0 or later

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due to dirty shutdown with High Write Speed mode"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might have changed. Verify that all recent configuration changes are still in effect.
```

- Cloud Volumes ONTAP 9.8 to 9.10.1

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might have changed. Verify that all recent configuration changes are still in effect.
```

When this happens, Cloud Volumes ONTAP should be able to boot up and continue to serve data without user intervention.

How to stop data access if data loss occurs

If you are concerned about data loss, want the applications to stop running upon data loss, and the data access to be resumed after the data loss issue is properly addressed, you can use the NVFAIL option from the CLI to achieve that goal.

To enable the NVFAIL option

```
vol modify -volume <vol-name> -nvfail on
```

To check NVFAIL settings

```
vol show -volume <vol-name> -fields nvfail
```

To disable the NVFAIL option

```
vol modify -volume <vol-name> -nvfail off
```

When data loss occurs, an NFS or iSCSI volume with NVFAIL enabled should stop serving data (there's no impact to CIFS which is a stateless protocol). For more details, refer to [How NVFAIL impacts access to NFS volumes or LUNs](#).

To check the NVFAIL state

```
vol show -fields in-nvfailed-state
```

After the data loss issue is properly addressed, you can clear the NVFAIL state and the volume will be available for data access.

To clear the NVFAIL state

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

Flash Cache

Some Cloud Volumes ONTAP configurations include local NVMe storage, which Cloud Volumes ONTAP uses as *Flash Cache* for better performance.

What's Flash Cache?

Flash Cache speeds access to data through real-time intelligent caching of recently read user data and NetApp metadata. It's effective for random read-intensive workloads, including databases, email, and file services.

Supported configurations

Flash Cache is supported with specific Cloud Volumes ONTAP configurations. View supported configurations in the [Cloud Volumes ONTAP Release Notes](#)

Limitations

- Compression must be disabled on all volumes to take advantage of the Flash Cache performance improvements.

Choose no storage efficiency when creating a volume from Cloud Manager, or create a volume and then [disable data compression by using the CLI](#).

- Cache rewarming after a reboot is not supported with Cloud Volumes ONTAP.

WORM storage

You can activate write once, read many (WORM) storage on a Cloud Volumes ONTAP system to retain files in unmodified form for a specified retention period. Cloud WORM storage is powered by SnapLock technology, which means WORM files are protected at the file level.

How WORM storage works

Once a file has been committed to WORM storage, it can't be modified, even after the retention period has expired. A tamper-proof clock determines when the retention period for a WORM file has elapsed.

After the retention period has elapsed, you are responsible for deleting any files that you no longer need.

Charging

Charging for WORM storage is hourly, according to the total provisioned capacity of WORM volumes.

[Learn about pricing for WORM storage.](#)

Activating WORM storage

You can activate WORM storage on a Cloud Volumes ONTAP system when you create a new working environment. This includes setting the default retention period for files.



You can't activate WORM storage on individual volumes—WORM must be activated at the system level.

The following image shows how to activate WORM storage when creating a working environment:

The screenshot shows the 'Create a New Working Environment' wizard in the Cloud Manager interface. The 'WORM (write once, read many)' step is active. On the left, under 'Write Speed', there are two options: 'Normal' (selected) and 'High'. The 'Normal' option description states: 'Data is written directly to disk, reducing the likelihood of data loss in the event of an unplanned system outage.' The 'High' option description states: 'Data is buffered in memory before it is written to disk, which provides faster write performance. Due to this caching, there is the potential for data loss in the event of an unplanned system outage.' On the right, under 'WORM', there is a description: 'You can use write once, read many (WORM) storage to retain critical files in unmodified form for regulatory and governance purposes and to protect from malware attacks. WORM files are protected at the file level. [Learn More](#)'. Below this, there are two radio buttons: 'Disable WORM' and 'Activate WORM' (selected). A notice states: 'Notice: If you activate WORM storage, data tiering to object storage will be disabled on the system.' At the bottom, there is a 'Retention Period' field set to '15' and a dropdown menu set to 'years'. A 'Continue' button is at the bottom center. The footer shows 'Cloud Manager 3.9.9 Build: 0 Jun 30, 2021 02:52:27 pm UTC Environment: staging'.

Committing files to WORM

You can use an application to commit files to WORM over NFS or CIFS, or use the ONTAP CLI to autocommit files to WORM automatically. You can also use a WORM appendable file to retain data that is written incrementally, like log information.

After you activate WORM storage on a Cloud Volumes ONTAP system, you must use the ONTAP CLI for all management of WORM storage. For instructions, refer to [ONTAP documentation](#).

Limitations

- WORM storage in Cloud Volumes ONTAP operates under a "trusted storage administrator" model. While WORM files are protected from alteration or modification, volumes can be deleted by a cluster administrator even if those volumes contain unexpired WORM data.
- In addition to the trusted storage administrator model, WORM storage in Cloud Volumes ONTAP also implicitly operates under a "trusted cloud administrator" model. A cloud administrator could delete WORM data before its expiry date by removing or editing cloud storage directly from the cloud provider.
- When WORM storage is activated, data tiering to object storage can't be enabled.

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.