NetApp

Storage

Cloud Volumes ONTAP

NetApp
January 13, 2023

Table of Contents

Storage

Client protocols

Cloud Volumes ONTAP supports the iSCSI, NFS, SMB, NVMe-TCP, 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. S3 protocol support enables you to configure S3 client access to objects contained in a bucket in a storage VM (SVM).

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

NVMe-TCP

NVMe-TCP is supported for cloud providers if you are using Cloud Volumes ONTAP version 9.12.1 or newer. BlueXP does not provide any management capabilities for NVMe-TCP.

For more information on configuring NVMe through ONTAP, see [Configure a storage VM for NVMe](#).

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 BlueXP. 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 BlueXP creates a 500 GiB aggregate, the usable capacity is 442.94 GiB.

Azure storage

In Azure, an aggregate can contain up to 12 disks that are all the same size. The disk type and maximum disk size depends on whether you use a single node system or an HA pair:

Single node systems

Single node systems can use three types of Azure Managed Disks:

- *Premium SSD Managed Disks* provide high performance for I/O-intensive workloads at a higher cost.
- *Standard SSD Managed Disks* provide consistent performance for workloads that require low IOPS.
- *Standard HDD Managed Disks* are a good choice if you don't need high IOPS and want to reduce your costs.

Each managed disk type has a maximum disk size of 32 TiB.

You can pair a managed disk with Azure Blob storage to tier inactive data to low-cost object storage.

HA pairs

HA pairs use two types of disks which provide high performance for I/O-intensive workloads at a higher cost:

- *Premium page blobs* with a maximum disk size of 8 TiB
- *Managed disks* with a maximum disk size of 32 TiB

Related links

- Microsoft Azure documentation: Azure managed disk types
- Microsoft Azure documentation: Overview of Azure page blobs
- Learn how to choose disk types and disk sizes for your systems in Azure
- Review storage limits for Cloud Volumes ONTAP in Azure

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.

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 Azure

When you enable data tiering in Azure, Cloud Volumes ONTAP uses Azure managed disks as a performance tier for hot data and Azure Blob storage as a capacity tier for inactive data.

Performance tier

The performance tier can be either SSDs or HDDs.

Capacity tier

A Cloud Volumes ONTAP system tiers inactive data to a single Blob container.

BlueXP creates a new storage account with a container for each Cloud Volumes ONTAP working environment. The name of the storage account is random. A different container is not created for each volume.

BlueXP creates the storage account with the following settings:

- Access tier: Hot
- Performance: Standard
- Redundancy: Locally-redundant storage (LRS)
- Account: StorageV2 (general purpose v2)
- Require secure transfer for REST API operations: Enabled
- Storage account key access: Enabled
- Minimum TLS version: Version 1.2
- Infrastructure encryption: Disabled

Storage access tiers

The default storage access tier for tiered data in Azure is the *hot* tier. The hot tier is ideal for frequently accessed data.

If you don't plan to access the inactive data, you can reduce your storage costs by changing to the *cool* storage tier. When you change the storage tier, inactive data starts in the hot storage tier and transitions to the cool storage tier, 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 tier. Learn more about Azure Blob storage access tiers.

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

The storage access tier 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.

BlueXP 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, BlueXP 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

BlueXP (formerly Cloud Manager) provides simplified and advanced management of Cloud Volumes ONTAP storage.

> ⚠️ All disks and aggregates must be created and deleted directly from BlueXP. 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

BlueXP 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. BlueXP creates aggregates for you when you launch an instance, and when you provision additional volumes.

When you create a volume, BlueXP 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.
- It purchases disks for a new aggregate and places the volume on that aggregate.

BlueXP 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.

Advanced allocation

Rather than let BlueXP 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 BlueXP notifies you of storage capacity decisions or whether BlueXP 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, BlueXP 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, BlueXP automatically purchases new disks for that aggregate so volumes can continue to grow.

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

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

  If BlueXP 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 provder in this scenario.

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

Management of LUNs with automatic capacity management

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

Manual capacity management

If the Account Admin set the Capacity Management Mode to manual, BlueXP 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

BlueXP 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.

Configurations that support high write speed

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

Azure

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

If you use an HA pair, Cloud Volumes ONTAP supports high write speed with several VM types, starting with the 9.8 release. Go to the Cloud Volumes ONTAP Release Notes to view the VM types that support high write speed.

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 9.12.1 or later

```
NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
```

- Cloud Volumes ONTAP 9.11.0 to 9.11.1

```
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 BlueXP, 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.

Activating WORM storage

How you activate WORM storage depends on the Cloud Volumes ONTAP version that you're using.

Version 9.10.1 and later

Starting with Cloud Volumes ONTAP 9.10.1, you have the option to enable or disable WORM at the volume level. How you choose to enable WORM depends on your needs.

When you create a new Cloud Volumes ONTAP working environment, you're prompted to enable or disable WORM storage:

- If you enable WORM storage when creating a working environment, every volume that you create from BlueXP has WORM enabled. But you can use System Manager or the CLI to create volumes that have WORM disabled.

  This option is a good choice if you want to create a dedicated system for WORM storage.

- If you disable WORM storage when creating a working environment, every volume that you create from BlueXP has WORM disabled. But you can use System Manager or the CLI to create volumes with WORM enabled.

  This option is a good choice if you want to mix different types of volumes on the same system.

With either option, you should understand how charging works.

Version 9.10.0 and earlier

You can activate WORM storage on a Cloud Volumes ONTAP system when you create a new working environment. You can't activate WORM storage on individual volumes—WORM must be activated at the system level. It can be activated only when you create the working environment.

Charging

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

You should understand the following charging behavior with Cloud Volumes ONTAP 9.10.1 and later:

- Beginning with ONTAP 9.10.1, WORM volumes and non-WORM volumes can exist on the same aggregate.
- If you enable WORM when you create a Cloud Volumes ONTAP working environment, every volume that you create from BlueXP has WORM enabled. However, you can use the ONTAP CLI or System Manager to create volumes that have WORM disabled. Those volumes are not charged at the WORM rate.
- If you don't enable WORM when you create a working environment, every volume that you create from BlueXP has WORM disabled. You are not charged at the WORM rate for those volumes. However, you can use the ONTAP CLI or System Manager to create WORM-enabled volumes. Those volumes will be charged at the WORM rate.

Learn about pricing for WORM storage

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.