NetApp

Cloud Volumes ONTAP documentation

Cloud Volumes ONTAP

NetApp
October 17, 2022

Table of Contents

Cloud Volumes ONTAP documentation

Release notes

What's new

Learn what's new with Cloud Volumes ONTAP management in Cloud Manager.

The enhancements described on this page are specific to Cloud Manager features that enable management of Cloud Volumes ONTAP. To learn what's new with the Cloud Volumes ONTAP software itself, go to the Cloud Volumes ONTAP Release Notes

18 September 2022

The following changes were introduced with the 3.9.22 release of the Connector.

Digital Wallet enhancements

- The Digital Wallet now shows a summary of the Optimized I/O licensing package and the provisioned WORM capacity for Cloud Volumes ONTAP systems across your account.

  These details can help you better understand how you're being charged and whether you need to purchase additional capacity.

  Learn how to view the consumed capacity in your account.

- You can now change from one charging method to the Optimized charging method.

  Learn how to change charging methods.

Optimize cost and performance

You can now optimize the cost and performance of a Cloud Volumes ONTAP system directly from the Canvas.

After you select a working environment, you can choose the **Optimize Cost & Performance** option to change the instance type for Cloud Volumes ONTAP. Choosing a smaller-sized instance can help you reduce costs, while changing to a larger-sized instance can help you optimize performance.

AutoSupport notifications

Cloud Manager will now generate a notification if a Cloud Volumes ONTAP system is unable to send AutoSupport messages. The notification includes a link to instructions that you can use to troubleshoot networking issues.

31 July 2022

The following changes were introduced with the 3.9.21 release of the Connector.

MTEKM license

The Multi-tenant Encryption Key Management (MTEKM) license is now included with new and existing Cloud Volumes ONTAP systems running version 9.11.1 or later.

Multi-tenant external key management enables individual storage VMs (SVMs) to maintain their own keys through a KMIP server when using NetApp Volume Encryption.

Learn how to encrypt volumes with NetApp encryption solutions.

Proxy server

Cloud Manager now automatically configures your Cloud Volumes ONTAP systems to use the Connector as a proxy server, if an outbound internet connection isn't available to send AutoSupport messages.

AutoSupport proactively monitors the health of your system and sends messages to NetApp technical support.

The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

Change charging method

You can now change the charging method for a Cloud Volumes ONTAP system that uses capacity-based licensing. For example, if you deployed a Cloud Volumes ONTAP system with the Essentials package, you can change it to the Professional package if your business needs changed. This feature is available from the Digital Wallet.

Learn how to change charging methods.

Security group enhancement

When you create a Cloud Volumes ONTAP working environment, the user interface now enables you to choose whether you want the predefined security group to allow traffic within the selected network only (recommended) or all networks.

18 July 2022

New licensing packages in Azure

Two new capacity-based licensing packages are available for Cloud Volumes ONTAP in Azure when you pay through an Azure Marketplace subscription:

- **Optimized**: Pay for provisioned capacity and I/O operations separately
- **Edge Cache**: Licensing for Cloud Volumes Edge Cache

Learn more about these licensing packages.

3 July 2022

The following changes were introduced with the 3.9.20 release of the Connector.

Digital Wallet

The Digital Wallet now shows you the total consumed capacity in your account and the consumed capacity by licensing package. This can help you understand how you're being charged and whether you need to purchase additional capacity.

Elastic Volumes enhancement

Cloud Manager now supports the Amazon EBS Elastic Volumes feature when creating a Cloud Volumes ONTAP working environment from the user interface. The Elastic Volumes feature is enabled by default when using gp3 or io1 disks. You can choose the initial capacity based on your storage needs and revise it after Cloud Volumes ONTAP is deployed.

Learn more about support for Elastic Volumes in AWS.

ONTAP S3 license in AWS

An ONTAP S3 license is now included on new and existing Cloud Volumes ONTAP systems running version 9.11.0 or later in AWS.

Learn how to configure and manage S3 object storage services in ONTAP

New Azure Cloud region support

Starting with the 9.10.1 release, Cloud Volumes ONTAP is now supported in the Azure West US 3 region.

View the full list of supported regions for Cloud Volumes ONTAP

ONTAP S3 license in Azure

An ONTAP S3 license is now included on new and existing Cloud Volumes ONTAP systems running version 9.9.1 or later in Azure.

Learn how to configure and manage S3 object storage services in ONTAP

7 June 2022

The following changes were introduced with the 3.9.19 release of the Connector.

Cloud Volumes ONTAP 9.11.1

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.11.1, which includes support for new features and additional cloud provider regions.

Learn about the new features included in this release of Cloud Volumes ONTAP

New Advanced View

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using ONTAP System Manager, which is a management interface that's provided with an ONTAP system. We have included the System Manager interface directly inside Cloud Manager so that you don't need to leave Cloud Manager for advanced management.

This Advanced View is available as a Preview with Cloud Volumes ONTAP 9.10.0 and later. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Learn more about the Advanced View.

Support for Amazon EBS Elastic Volumes

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.

Support for Elastic Volumes is available starting with *new* Cloud Volumes ONTAP 9.11.0 systems and with gp3 and io1 EBS disk types.

Learn more about support for Elastic Volumes.

Note that support for Elastic Volumes requires new AWS permissions for the Connector:

```
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
```

Be sure to provide these permissions to each set of AWS credentials that you've added to Cloud Manager. View the latest Connector policy for AWS.

Support for deploying HA pairs in shared AWS subnets

Cloud Volumes ONTAP 9.11.1 includes support for AWS VPC sharing. This release of the Connector enables you to deploy an HA pair in an AWS shared subnet when using the API.

Learn how to deploy an HA pair in a shared subnet.

Limited network access when using service endpoints

Cloud Manager now limits network access when using a VNet service endpoint for connections between Cloud Volumes ONTAP and storage accounts. Cloud Manager uses a service endpoint if you disable Azure Private Link connections.

Learn more about Azure Private Link connections with Cloud Volumes ONTAP.

Support for creating storage VMs in Google Cloud

Multiple storage VMs are now supported with Cloud Volumes ONTAP in Google Cloud, starting with the 9.11.1 release. Starting with this release of the Connector, Cloud Manager enables you to create storage VMs on Cloud Volumes ONTAP HA pairs in Google Cloud by using the API.

Support for creating storage VMs requires new Google Cloud permissions for the Connector:

```
 - compute.instanceGroups.get
 - compute.addresses.get
```

Note that you must use the ONTAP CLI or System Manager to create a storage VM on a single node system.

- Learn more about storage VM limits in Google Cloud
- Learn how to create data-serving storage VMs for Cloud Volumes ONTAP in Google Cloud

2 May 2022

The following changes were introduced with the 3.9.18 release of the Connector.

Cloud Volumes ONTAP 9.11.0

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.11.0.

Learn about the new features included in this release of Cloud Volumes ONTAP.

Enhancement to mediator upgrades

When Cloud Manager upgrades the mediator for an HA pair, it now validates that a new mediator image is available before it deletes the boot disk. This change ensures that the mediator can continue to operate successfully if the upgrade process is unsuccessful.

K8s tab has been removed

The K8s tab was deprecated in a previous and has now been removed. If you want to use Kubernetes with Cloud Volumes ONTAP, you can add managed-Kubernetes clusters to the Canvas as a working environment for advanced data management.

Learn about Kubernetes data management in Cloud Manager

Annual contract in Azure

The Essentials and Professional packages are now available in Azure through an annual contract. You can contact your NetApp sales representative to purchase an annual contract. The contract is available as a private

offer in the Azure Marketplace.

After NetApp shares the private offer with you, you can select the annual plan when you subscribe from the Azure Marketplace during working environment creation.

[Learn more about licensing](#).

S3 Glacier Instant Retrieval

You can now store tiered data in the Amazon S3 Glacier Instant Retrieval storage class.

[Learn how to change the storage class for tiered data](#).

New AWS permissions required for the Connector

The following permissions are now required to create an AWS spread placement group when deploying an HA pair in a single Availability Zone (AZ):

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

These permissions are now required to optimize how Cloud Manager creates the placement group.

Be sure to provide these permissions to each set of AWS credentials that you've added to Cloud Manager. [View the latest Connector policy for AWS](#).

New Google Cloud region support

Cloud Volumes ONTAP is now supported in the following Google Cloud regions starting with the 9.10.1 release:

- Delhi (asia-south2)
- Melbourne (australia-southeast2)
- Milan (europe-west8) - single node only
- Santiago (southamerica-west1) - single node only

[View the full list of supported regions for Cloud Volumes ONTAP](#)

Support for n2-standard-16 in Google Cloud

The n2-standard-16 machine type is now supported with Cloud Volumes ONTAP in Google Cloud, starting with the 9.10.1 release.

[View supported configurations for Cloud Volumes ONTAP in Google Cloud](#)

Enhancements to Google Cloud firewall policies

- When you create a Cloud Volumes ONTAP HA pair in Google Cloud, Cloud Manager will now display all existing firewall policies in a VPC.

  Previously, Cloud Manager wouldn't display any policies in VPC-1, VPC-2, or VPC-3 that didn't have a target tag.

- When you create a Cloud Volumes ONTAP single node system in Google Cloud, you can now choose whether you want the predefined firewall policy to allow traffic within the selected VPC only (recommended) or all VPCs.

Enhancement to Google Cloud service accounts

When you select the Google Cloud service account to use with Cloud Volumes ONTAP, Cloud Manager now displays the email address that's associated with each service account. Viewing the email address can make it easier to distinguish between service accounts that share the same name.
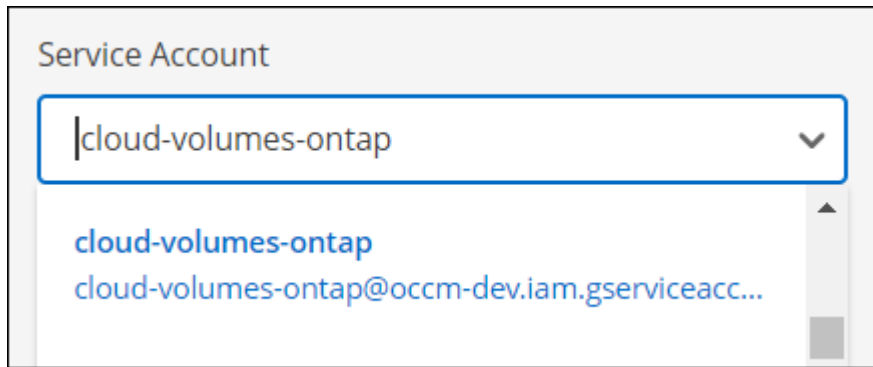
3 April 2022

System Manager link has been removed

We have removed the System Manager link that was previously available from within a Cloud Volumes ONTAP working environment.

You can still connect to System Manager by entering the cluster management IP address in a web browser that has a connection to the Cloud Volumes ONTAP system. Learn more about connecting to System Manager.

Charging for WORM storage

Now that the introductory special rate has expired, you will now be charged for using WORM storage. Charging is hourly, according to the total provisioned capacity of WORM volumes. This applies to new and existing Cloud Volumes ONTAP systems.

Learn about pricing for WORM storage.

27 February 2022

The following changes were introduced with the 3.9.16 release of the Connector.

Redesigned volume wizard

The create new volume wizard that we recently introduced is now available when creating a volume on a specific aggregate from the **Advanced allocation** option.

Learn how to create volumes on a specific aggregate.

9 February 2022

Marketplace updates

- The Essentials package and Professional package are now available in all cloud provider marketplaces.

  These by-capacity charging methods enable you to pay by the hour or to purchase an annual contract directly from your cloud provider. You still have the option to purchase a by-capacity license directly from NetApp.

  If you have an existing subscription in a cloud marketplace, you're automatically subscribed to these new offerings as well. You can choose by-capacity charging when you deploy a new Cloud Volumes ONTAP working environment.

  If you're a new customer, Cloud Manager will prompt you to subscribe when you create a new working environment.

- By-node licensing from all cloud provider marketplaces is deprecated and no longer available for new subscribers. This includes annual contracts and hourly subscriptions (Explore, Standard, and Premium).

  This charging method is still available for existing customers who have an active subscription.

Learn more about the licensing options for Cloud Volumes ONTAP.

6 February 2022

Exchange unassigned licenses

If you have an unassigned node-based license for Cloud Volumes ONTAP that you haven't used, you can now exchange the license by converting it to a Cloud Backup license, Cloud Data Sense license, or Cloud Tiering license.

This action revokes the Cloud Volumes ONTAP license and creates a dollar-equivalent license for the service with the same expiry date.

Learn how to exchange unassigned node-based licenses.

30 January 2022

The following changes were introduced with the 3.9.15 release of the Connector.

Redesigned licensing selection

We redesigned the licensing selection screen when creating a new Cloud Volumes ONTAP working environment. The changes highlight the by-capacity charging methods that were introduced in July 2021 and support upcoming offerings through the cloud provider marketplaces.

Digital Wallet update

We updated the **Digital Wallet** by consolidating Cloud Volumes ONTAP licenses in a single tab.

2 January 2022

The following changes were introduced with the 3.9.14 release of the Connector.

Support for additional Azure VM types

Cloud Volumes ONTAP is now supported with the following VM types in Microsoft Azure, starting with the 9.10.1 release:

- E4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

Go to the Cloud Volumes ONTAP Release Notes for more details about supported configurations.

FlexClone charging update

If you use a capacity-based license for Cloud Volumes ONTAP, you are no longer charged for the capacity used by FlexClone volumes.

Charging method now displayed

Cloud Manager now shows the charging method for each Cloud Volumes ONTAP working environment in the right panel of the Canvas.

Choose your user name

When you create a Cloud Volumes ONTAP working environment, you now have the option to enter your preferred user name, instead of the default admin user name.

Volume creation enhancements

We made a few enhancements to volume creation:

- We redesigned the create volume wizard for ease of use.
- Tags that you add to a volume are now associated with the Application Templates service, which can help you organize and simplify the management of your resources.
- You can now choose a custom export policy for NFS.

28 November 2021

The following changes were introduced with the 3.9.13 release of the Connector.

Cloud Volumes ONTAP 9.10.1

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.10.1.

Learn about the new features included in this release of Cloud Volumes ONTAP.

Keystone Flex Subscriptions

You can now use Keystone Flex Subscriptions to pay for Cloud Volumes ONTAP HA pairs.

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service that delivers a seamless hybrid cloud experience for those preferring OpEx consumption models to upfront CapEx or leasing.

A Keystone Flex Subscription is supported with all new versions of Cloud Volumes ONTAP that you can deploy from Cloud Manager.

- Learn more about Keystone Flex Subscriptions.
- Learn how to get started with Keystone Flex Subscriptions in Cloud Manager.

Port reduction

Ports 8023 and 49000 are no longer open on Cloud Volumes ONTAP systems in Azure for both single node systems and HA pairs.

This change applies to *new* Cloud Volumes ONTAP systems starting with the 3.9.13 release of the Connector.

4 October 2021

The following changes were introduced with the 3.9.11 release of the Connector.

Cloud Volumes ONTAP 9.10.0

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.10.0.

Learn about the new features included in this release of Cloud Volumes ONTAP.

Reduced deployment time

We reduced the amount of time that it takes to deploy a Cloud Volumes ONTAP working environment in Microsoft Azure or in Google Cloud when normal write speed is enabled. The deployment time is now 3-4 minutes shorter on average.

2 September 2021

The following changes were introduced with the 3.9.10 release of the Connector.

Customer-managed encryption key in Azure

Data is automatically encrypted on Cloud Volumes ONTAP in Azure using Azure Storage Service Encryption with a Microsoft-managed key. But you can now use your own customer-managed encryption key instead by completing the following steps:

1. From Azure, create a key vault and then generate a key in that vault.
2. From Cloud Manager, use the API to create a Cloud Volumes ONTAP working environment that uses the key.

Learn more about these steps.

7 July 2021

The following changes were introduced with the 3.9.8 release of the Connector.

New charging methods

New charging methods are available for Cloud Volumes ONTAP.

- **Capacity-based BYOL**: A capacity-based license enables you to pay for Cloud Volumes ONTAP per TiB of capacity. The license is associated with your NetApp account and enables you to create as multiple Cloud Volumes ONTAP systems, as long as enough capacity is available through your license. Capacity-based licensing is available in the form of a package, either *Essentials* or *Professional*.

- **Freemium offering**: Freemium enables you to use all Cloud Volumes ONTAP features free of charge from NetApp (cloud provider charges still apply). You're limited to 500 GiB of provisioned capacity per system and there's no support contract. You can have up to 10 Freemium systems.

Learn more about these licensing options.

Here's an example of the charging methods that you can choose from:
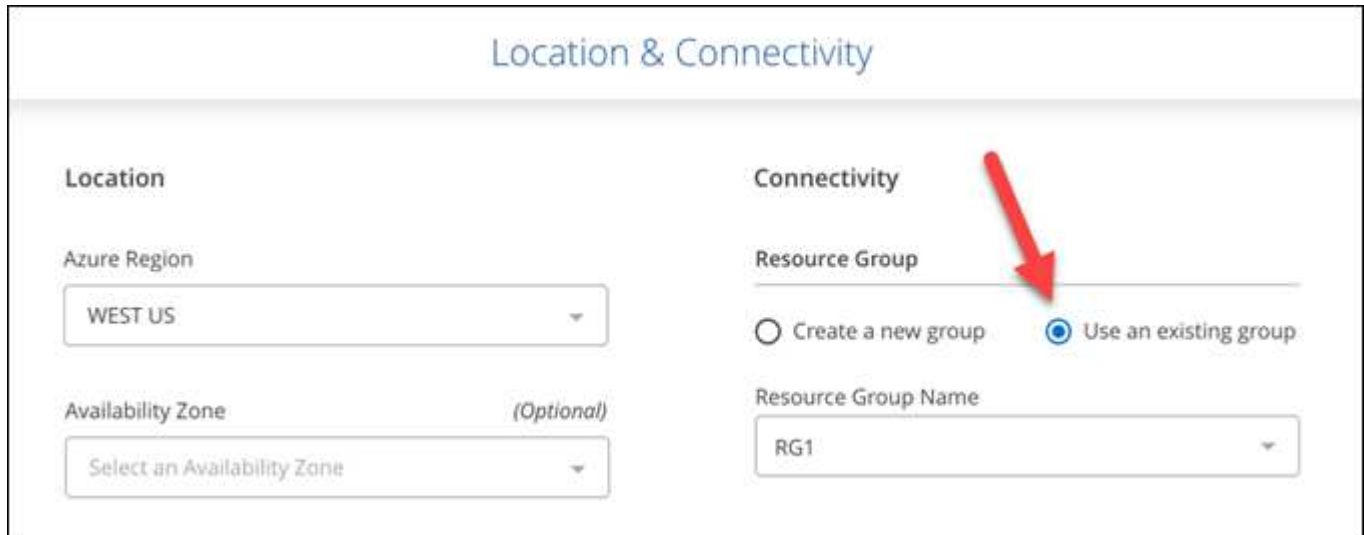
WORM storage available for general use

Write once, read many (WORM) storage is no longer in Preview and is now available for general use with Cloud Volumes ONTAP. Learn more about WORM storage.

Select existing Azure resource groups

When creating a Cloud Volumes ONTAP system in Azure, you now have the option to select an existing resource group for the VM and its associated resources.

The following permissions enable Cloud Manager to remove Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion:

```
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
```

Be sure to provide these permissions to each set of Azure credentials that you've added to Cloud Manager. View the latest Connector policy for Azure.

Blob public access now disabled in Azure

As a security enhancement, Cloud Manager now disables **Blob public access** when creating a storage account for Cloud Volumes ONTAP.

Azure Private Link enhancement

By default, Cloud Manager now enables an Azure Private Link connection on the boot diagnostics storage account for new Cloud Volumes ONTAP systems.

This means *all* storage accounts for Cloud Volumes ONTAP will now use a private link.

Learn more about using an Azure Private Link with Cloud Volumes ONTAP.

30 May 2021

The following changes were introduced with the 3.9.7 release of the Connector.

Minimum cooling period for auto tiering policy

If you enabled data tiering on a volume using the *auto* tiering policy, you can now adjust the minimum cooling period using the API.

[Learn how to adjust the minimum cooling period.](#)

Enhancement to custom export policies

When you create a new NFS volume, Cloud Manager now displays custom export policies in ascending order, making it easier for you to find the export policy that you need.

Deletion of old cloud snapshots

Cloud Manager now deletes older cloud snapshots of root and boot disks that are created when a Cloud Volumes ONTAP system is deployed and every time its powered down. Only the two most recent snapshots are retained for both the root and boot volumes.

This enhancement helps reduce cloud provider costs by removing snapshots that are no longer needed.

Note that a Connector requires a new permission to delete Azure snapshots. [View the latest Connector policy for Azure](#).

```
"Microsoft.Compute/snapshots/delete"
```

24 May 2021

Cloud Volumes ONTAP 9.9.1

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.9.1.

[Learn about the new features included in this release of Cloud Volumes ONTAP](#).

11 Apr 2021

The following changes were introduced with the 3.9.5 release of the Connector.

Logical space reporting

Cloud Manager now enables logical space reporting on the initial storage VM that it creates for Cloud Volumes ONTAP.

When space is reported logically, ONTAP reports the volume space such that all the physical space saved by the storage efficiency features are also reported as used.

TLS 1.2 for Azure storage accounts

When Cloud Manager creates storage accounts in Azure for Cloud Volumes ONTAP, the TLS version for the storage account is now version 1.2.

8 Mar 2021

The following changes were introduced with the 3.9.4 release of the Connector.

Cloud Volumes ONTAP 9.9.0

Cloud Manager can now deploy and manage Cloud Volumes ONTAP 9.9.0.

Learn about the new features included in this release of Cloud Volumes ONTAP.

Support for Azure DoD

You can now deploy Cloud Volumes ONTAP 9.8 in the Azure Department of Defense (DoD) Impact Level 6 (IL6).

4 Jan 2021

The following changes were introduced with the 3.9.2 release of the Connector.
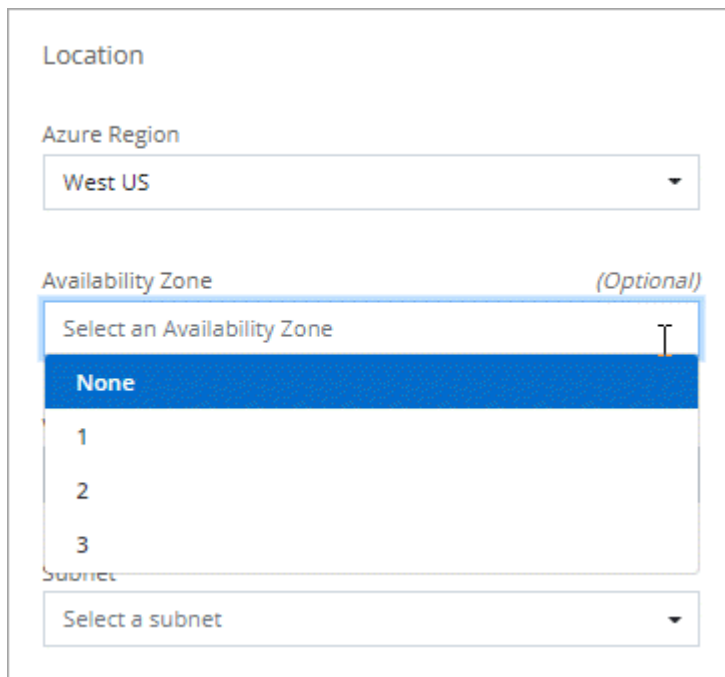
Ultra SSD VNVRAM in supported Azure regions

Cloud Volumes ONTAP can now use an Ultra SSD as VNVRAM when you use the E32s_v3 VM type with a single node system in any supported Azure region.

VNVRAM provides better write performance.

Choose an Availability Zone in Azure

You can now choose the Availability Zone in which you'd like to deploy a single node Cloud Volumes ONTAP system. If you don't select an AZ, Cloud Manager will select one for you.

3 Nov 2020

The following changes were introduced with the 3.9.0 release of the Connector.

Azure Private Link for Cloud Volumes ONTAP

By default, Cloud Manager now enables an Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts. A Private Link secures connections between endpoints in Azure.

- Learn more about Azure Private Links
- Learn more about using an Azure Private Link with Cloud Volumes ONTAP

Known limitations

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

These limitations are specific to Cloud Volumes ONTAP management in Cloud Manager. To view limitations with the Cloud Volumes ONTAP software itself, go to the Cloud Volumes ONTAP Release Notes

Cloud Manager doesn't support FlexGroup volumes

While Cloud Volumes ONTAP supports FlexGroup volumes, Cloud Manager does not. If you create a FlexGroup volume from System Manager or from the CLI, then you should set Cloud Manager's Capacity Management mode to Manual. Automatic mode might not work properly with FlexGroup volumes.

Cloud Manager doesn't support S3 with Cloud Volumes ONTAP

While Cloud Volumes ONTAP supports S3 as an option for scale-out storage in some cloud providers, Cloud Manager doesn't provide any management capabilities for this feature. Using the CLI is the best practice to configure S3 client access from Cloud Volumes ONTAP. For details, refer to the S3 Configuration Power Guide.

Learn more about Cloud Volumes ONTAP support for S3 and other client protocols.

Cloud Manager doesn't support disaster recovery for storage VMs

Cloud Manager doesn't provide any setup or orchestration support for storage VM disaster recovery. You must use System Manager or the CLI.

- SVM Disaster Recovery Preparation Express Guide
- SVM Disaster Recovery Express Guide

Cloud Volumes ONTAP Release Notes

The Release Notes for Cloud Volumes ONTAP provide release-specific information. What's new in the release, supported configurations, storage limits, and any known limitations or issues that can affect product functionality.

Go to the Cloud Volumes ONTAP Release Notes

Get started

Learn about Cloud Volumes ONTAP

Cloud Volumes ONTAP enables you to optimize your cloud storage costs and performance while enhancing data protection, security, and compliance.

Cloud Volumes ONTAP is a software-only storage appliance that runs ONTAP data management software in the cloud. It provides enterprise-grade storage with the following key features:

- Storage efficiencies

  Leverage built-in data deduplication, data compression, thin provisioning, and cloning to minimize storage costs.

- High availability

  Ensure enterprise reliability and continuous operations in case of failures in your cloud environment.

- Data protection

  Cloud Volumes ONTAP leverages SnapMirror, NetApp's industry-leading replication technology, to replicate on-premises data to the cloud so it's easy to have secondary copies available for multiple use cases.

  Cloud Volumes ONTAP also integrates with Cloud Backup to deliver backup and restore capabilities for protection, and long-term archive of your cloud data.

  Learn more about Cloud Backup

- Data tiering

  Switch between high and low-performance storage pools on-demand without taking applications offline.

- Application consistency

  Ensure consistency of NetApp Snapshot copies using NetApp SnapCenter.

  Learn more about SnapCenter

- Data security

  Cloud Volumes ONTAP supports data encryption and provides protection against viruses and ransomware.

- Privacy compliance controls

  Integration with Cloud Data Sense helps you understand data context and identify sensitive data.

  Learn more about Cloud Data Sense

ⓘ   Licenses for ONTAP features are included with Cloud Volumes ONTAP.

View supported Cloud Volumes ONTAP configurations

19

Learn more about Cloud Volumes ONTAP

Get started in Microsoft Azure

Quick start for Cloud Volumes ONTAP in Azure

Get started with Cloud Volumes ONTAP for Azure in a few steps.

1   **Create a Connector**

If you don't have a Connector yet, an Account Admin needs to create one. Learn how to create a Connector in Azure.

When you create your first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to deploy a Connector if you don't have one yet.

2   **Plan your configuration**

Cloud Manager offers preconfigured packages that match your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you. Learn more.

3   **Set up your networking**

a. Ensure that your VNet and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.

b. Enable outbound internet access from the target VNet so the Connector and Cloud Volumes ONTAP can contact several endpoints.

This step is important because the Connector can't manage Cloud Volumes ONTAP without outbound internet access. If you need to limit outbound connectivity, refer to the list of endpoints for the Connector and Cloud Volumes ONTAP.

Learn more about networking requirements.

4   **Launch Cloud Volumes ONTAP using Cloud Manager**

Click **Add Working Environment**, select the type of system that you would like to deploy, and complete the steps in the wizard. Read step-by-step instructions.

Related links

- Creating a Connector from Cloud Manager
- Creating a Connector from the Azure Marketplace
- Installing the Connector software on a Linux host
- What Cloud Manager does with permissions

Plan your Cloud Volumes ONTAP configuration in Azure

When you deploy Cloud Volumes ONTAP in Azure, you can choose a preconfigured system that matches your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you.

Choose a Cloud Volumes ONTAP license

Several licensing options are available for Cloud Volumes ONTAP. Each option enables you to choose a consumption model that meets your needs.

- Learn about licensing options for Cloud Volumes ONTAP
- Learn how to set up licensing

Choose a supported region

Cloud Volumes ONTAP is supported in most Microsoft Azure regions. View the full list of supported regions.

Choose a supported VM type

Cloud Volumes ONTAP supports several VM types, depending on the license type that you choose.

Supported configurations for Cloud Volumes ONTAP in Azure

Understand storage limits

The raw capacity limit for a Cloud Volumes ONTAP system is tied to the license. Additional limits impact the size of aggregates and volumes. You should be aware of these limits as you plan your configuration.

Storage limits for Cloud Volumes ONTAP in Azure

Size your system in Azure

Sizing your Cloud Volumes ONTAP system can help you meet requirements for performance and capacity. You should be aware of a few key points when choosing a VM type, disk type, and disk size:

Virtual machine type

Look at the supported virtual machine types in the Cloud Volumes ONTAP Release Notes and then review details about each supported VM type. Be aware that each VM type supports a specific number of data disks.

- Azure documentation: General purpose virtual machine sizes
- Azure documentation: Memory optimized virtual machine sizes

Azure disk type

When you create volumes for Cloud Volumes ONTAP, you need to choose the underlying cloud storage that Cloud Volumes ONTAP uses as a disk.

HA systems use Premium page blobs. Meanwhile, single node systems can use two 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.

  For additional details about the use cases for these disks, see Microsoft Azure Documentation: What disk types are available in Azure?.

Azure disk size

When you launch Cloud Volumes ONTAP instances, you must choose the default disk size for aggregates. Cloud Manager uses this disk size for the initial aggregate, and for any additional aggregates that it creates when you use the simple provisioning option. You can create aggregates that use a disk size different from the default by using the advanced allocation option.

> All disks in an aggregate must be the same size.

When choosing a disk size, you should take several factors into consideration. The disk size impacts how much you pay for storage, the size of volumes that you can create in an aggregate, the total capacity available to Cloud Volumes ONTAP, and storage performance.

The performance of Azure Premium Storage is tied to the disk size. Larger disks provide higher IOPS and throughput. For example, choosing 1 TiB disks can provide better performance than 500 GiB disks, at a higher cost.

There are no performance differences between disk sizes for Standard Storage. You should choose disk size based on the capacity that you need.

Refer to Azure for IOPS and throughput by disk size:

- Microsoft Azure: Managed Disks pricing
- Microsoft Azure: Page Blobs pricing

View default system disks

In addition to the storage for user data, Cloud Manager also purchases cloud storage for Cloud Volumes ONTAP system data (boot data, root data, core data, and NVRAM). For planning purposes, it might help for you to review these details before you deploy Cloud Volumes ONTAP.

View the default disks for Cloud Volumes ONTAP system data in Azure.

> The Connector also requires a system disk. View details about the Connector's default configuration.

Collect networking information

When you deploy Cloud Volumes ONTAP in Azure, you need to specify details about your virtual network. You can use a worksheet to collect the information from your administrator.

Azure information	Your value
Region	

Azure information	Your value
Virtual network (VNet)	
Subnet	
Network security group (if using your own)	

Choose a write speed

Cloud Manager enables you to choose a write speed setting for Cloud Volumes ONTAP. 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. Learn more about write speed.

Choose a volume usage profile

ONTAP includes several storage efficiency features that can reduce the total amount of storage that you need. When you create a volume in Cloud Manager, you can choose a profile that enables these features or a profile that disables them. You should learn more about these features to help you decide which profile to use.

NetApp storage efficiency features provide the following benefits:

Thin provisioning

Presents more logical storage to hosts or users than you actually have in your physical storage pool. Instead of preallocating storage space, storage space is allocated dynamically to each volume as data is written.

Deduplication

Improves efficiency by locating identical blocks of data and replacing them with references to a single shared block. This technique reduces storage capacity requirements by eliminating redundant blocks of data that reside in the same volume.

Compression

Reduces the physical capacity required to store data by compressing data within a volume on primary, secondary, and archive storage.

Networking requirements for Cloud Volumes ONTAP in Azure

Set up your Azure networking so Cloud Volumes ONTAP systems can operate properly. This includes networking for the Connector and Cloud Volumes ONTAP.

Requirements for Cloud Volumes ONTAP

The following networking requirements must be met in Azure.

Outbound internet access

Cloud Volumes ONTAP nodes require outbound internet access for NetApp AutoSupport, which proactively monitors the health of your system and sends messages to NetApp technical support.

Routing and firewall policies must allow HTTP/HTTPS traffic to the following endpoints so Cloud Volumes ONTAP can send AutoSupport messages:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

If an outbound internet connection isn't available to send AutoSupport messages, Cloud Manager automatically configures your Cloud Volumes ONTAP systems to use the Connector as a proxy server. The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you defined strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

After you've verified that outbound internet access is available, you can test AutoSupport to ensure that it can send messages. For instructions, refer to ONTAP docs: Set up AutoSupport.

If Cloud Manager notifies you that AutoSupport messages can't be sent, troubleshoot your AutoSupport configuration.

IP addresses

Cloud Manager allocates the following number of IP addresses to Cloud Volumes ONTAP in Azure:

- Single node: 5 IP addresses
- HA pair: 16 IP addresses

Note that Cloud Manager creates an SVM management LIF on HA pairs, but not on single node systems in Azure.

> A LIF is an IP address associated with a physical port. An SVM management LIF is required for management tools like SnapCenter.

Secure connections to Azure services

By default, Cloud Manager enables an Azure Private Link for connections between Cloud Volumes ONTAP and Azure storage accounts.

In most cases, there's nothing that you need to do—Cloud Manager manages the Azure Private Link for you. But if you use Azure Private DNS, then you'll need to edit a configuration file. You should also be aware of a requirement for the Connector location in Azure.

You can also disable the Private Link connection, if required by your business needs. If you disable the link, Cloud Manager configures Cloud Volumes ONTAP to use a service endpoint instead.

Learn more about using Azure Private Links or service endpoints with Cloud Volumes ONTAP.

Connections to other ONTAP systems

To replicate data between a Cloud Volumes ONTAP system in Azure and ONTAP systems in other networks, you must have a VPN connection between the Azure VNet and the other network—for example, your corporate network.

For instructions, refer to Microsoft Azure Documentation: Create a Site-to-Site connection in the Azure portal.

Port for the HA interconnect

A Cloud Volumes ONTAP HA pair includes an HA interconnect, which allows each node to continually check whether its partner is functioning and to mirror log data for the other's nonvolatile memory. The HA interconnect uses TCP port 10006 for communication.

By default, communication between the HA interconnect LIFs is open and there are no security group rules for this port. But if you create a firewall between the HA interconnect LIFs, then you need to ensure that TCP traffic is open for port 10006 so that the HA pair can operate properly.

Only one HA pair in an Azure resource group

You must use a *dedicated* resource group for each Cloud Volumes ONTAP HA pair that you deploy in Azure. Only one HA pair is supported in a resource group.

Cloud Manager experiences connection issues if you try to deploy a second Cloud Volumes ONTAP HA pair in an Azure resource group.

Security groups

You don't need to create security groups because Cloud Manager does that for you. If you need to use your own, refer to the security group rules listed below.

Security group rules

Cloud Manager creates Azure security groups that include the inbound and outbound rules that Cloud Volumes ONTAP needs to operate successfully. You might want to refer to the ports for testing purposes or if you prefer your to use own security groups.

The security group for Cloud Volumes ONTAP requires both inbound and outbound rules.

Inbound rules for single node systems

When you create a working environment and choose a predefined security group, you can choose to allow traffic within one of the following:

- **Selected VNet only**: the source for inbound traffic is the subnet range of the VNet for the Cloud Volumes ONTAP system and the subnet range of the VNet where the Connector resides. This is the recommended option.
- **All VNets**: the source for inbound traffic is the 0.0.0.0/0 IP range.

Priority and name	Port and protocol	Source and destination	Description
1000 inbound_ssh	22 TCP	Any to Any	SSH access to the IP address of the cluster management LIF or a node management LIF
1001 inbound_http	80 TCP	Any to Any	HTTP access to the System Manager web console using the IP address of the cluster management LIF
1002 inbound_111_tcp	111 TCP	Any to Any	Remote procedure call for NFS
1003 inbound_111_udp	111 UDP	Any to Any	Remote procedure call for NFS

Priority and name	Port and protocol	Source and destination	Description
1004 inbound_139	139 TCP	Any to Any	NetBIOS service session for CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Any to Any	Simple network management protocol
1006 inbound_161-162 _udp	161-162 UDP	Any to Any	Simple network management protocol
1007 inbound_443	443 TCP	Any to Any	Connectivity with the Connector and HTTPS access to the System Manager web console using the IP address of the cluster management LIF
1008 inbound_445	445 TCP	Any to Any	Microsoft SMB/CIFS over TCP with NetBIOS framing
1009 inbound_635_tcp	635 TCP	Any to Any	NFS mount
1010 inbound_635_udp	635 UDP	Any to Any	NFS mount
1011 inbound_749	749 TCP	Any to Any	Kerberos
1012 inbound_2049_tcp	2049 TCP	Any to Any	NFS server daemon
1013 inbound_2049_udp	2049 UDP	Any to Any	NFS server daemon
1014 inbound_3260	3260 TCP	Any to Any	iSCSI access through the iSCSI data LIF
1015 inbound_4045-4046_tcp	4045-4046 TCP	Any to Any	NFS lock daemon and network status monitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Any to Any	NFS lock daemon and network status monitor
1017 inbound_10000	10000 TCP	Any to Any	Backup using NDMP
1018 inbound_11104-11105	11104-11105 TCP	Any to Any	SnapMirror data transfer
3000 inbound_deny _all_tcp	Any port TCP	Any to Any	Block all other TCP inbound traffic

Priority and name	Port and protocol	Source and destination	Description
3001 inbound_deny_all_udp	Any port UDP	Any to Any	Block all other UDP inbound traffic
65000 AllowVnetInBound	Any port Any protocol	VirtualNetwork to VirtualNetwork	Inbound traffic from within the VNet
65001 AllowAzureLoad BalancerInBound	Any port Any protocol	AzureLoadBalancer to Any	Data traffic from the Azure Standard Load Balancer
65500 DenyAllInBound	Any port Any protocol	Any to Any	Block all other inbound traffic

Inbound rules for HA systems

When you create a working environment and choose a predefined security group, you can choose to allow traffic within one of the following:

- **Selected VNet only**: the source for inbound traffic is the subnet range of the VNet for the Cloud Volumes ONTAP system and the subnet range of the VNet where the Connector resides. This is the recommended option.
- **All VNets**: the source for inbound traffic is the 0.0.0.0/0 IP range.

> (i) HA systems have less inbound rules than single node systems because inbound data traffic goes through the Azure Standard Load Balancer. Because of this, traffic from the Load Balancer should be open, as shown in the "AllowAzureLoadBalancerInBound" rule.

Priority and name	Port and protocol	Source and destination	Description
100 inbound_443	443 Any protocol	Any to Any	Connectivity with the Connector and HTTPS access to the System Manager web console using the IP address of the cluster management LIF
101 inbound_111_tcp	111 Any protocol	Any to Any	Remote procedure call for NFS
102 inbound_2049_tcp	2049 Any protocol	Any to Any	NFS server daemon
111 inbound_ssh	22 Any protocol	Any to Any	SSH access to the IP address of the cluster management LIF or a node management LIF
121 inbound_53	53 Any protocol	Any to Any	DNS and CIFS

Priority and name	Port and protocol	Source and destination	Description
65000 AllowVnetInBound	Any port Any protocol	VirtualNetwork to VirtualNetwork	Inbound traffic from within the VNet
65001 AllowAzureLoad BalancerInBound	Any port Any protocol	AzureLoadBalan cer to Any	Data traffic from the Azure Standard Load Balancer
65500 DenyAllInBound	Any port Any protocol	Any to Any	Block all other inbound traffic

Outbound rules

The predefined security group for Cloud Volumes ONTAP opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for Cloud Volumes ONTAP includes the following outbound rules.

Port	Protocol	Purpose
All	All TCP	All outbound traffic
All	All UDP	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by Cloud Volumes ONTAP.

ⓘ The source is the interface (IP address) on the Cloud Volumes ONTAP system.

Service	Port	Protocol	Source	Destination	Purpose
Active Directory	88	TCP	Node management LIF	Active Directory forest	Kerberos V authentication
	137	UDP	Node management LIF	Active Directory forest	NetBIOS name service
	138	UDP	Node management LIF	Active Directory forest	NetBIOS datagram service
	139	TCP	Node management LIF	Active Directory forest	NetBIOS service session
	389	TCP & UDP	Node management LIF	Active Directory forest	LDAP
	445	TCP	Node management LIF	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	464	TCP	Node management LIF	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	464	UDP	Node management LIF	Active Directory forest	Kerberos key administration
	749	TCP	Node management LIF	Active Directory forest	Kerberos V change & set Password (RPCSEC_GSS)
	88	TCP	Data LIF (NFS, CIFS, iSCSI)	Active Directory forest	Kerberos V authentication
	137	UDP	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS name service
	138	UDP	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS datagram service
	139	TCP	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS service session
	389	TCP & UDP	Data LIF (NFS, CIFS)	Active Directory forest	LDAP
	445	TCP	Data LIF (NFS, CIFS)	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	464	TCP	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	464	UDP	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos key administration
	749	TCP	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos V change & set password (RPCSEC_GSS)

Service	Port	Protocol	Source	Destination	Purpose
AutoSupport	HTTPS	443	Node management LIF	support.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	support.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Connector	Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available
DHCP	68	UDP	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	67	UDP	Node management LIF	DHCP	DHCP server
DNS	53	UDP	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	Node management LIF	Destination servers	NDMP copy
SMTP	25	TCP	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	161	TCP	Node management LIF	Monitor server	Monitoring by SNMP traps
	161	UDP	Node management LIF	Monitor server	Monitoring by SNMP traps
	162	TCP	Node management LIF	Monitor server	Monitoring by SNMP traps
	162	UDP	Node management LIF	Monitor server	Monitoring by SNMP traps
SnapMirror	11104	TCP	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	11105	TCP	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
Syslog	514	UDP	Node management LIF	Syslog server	Syslog forward messages

Requirements for the Connector

Set up your networking so that the Connector can manage resources and processes within your public cloud environment. The most important step is ensuring outbound internet access to various endpoints.

> 💡 If your network uses a proxy server for all communication to the internet, you can specify the proxy server from the Settings page. Refer to Configuring the Connector to use a proxy server.

Connections to target networks

A Connector requires a network connection to the VPCs and VNets in which you want to deploy Cloud Volumes ONTAP.

For example, if you install a Connector in your corporate network, then you must set up a VPN connection to the VPC or VNet in which you launch Cloud Volumes ONTAP.

Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment.

Endpoints	Purpose
https://support.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	To provide SaaS features and services within Cloud Manager.
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	To upgrade the Connector and its Docker components.

Security group rules

The security group for the Connector requires both inbound and outbound rules.

Inbound rules

Port	Protocol	Purpose
22	SSH	Provides SSH access to the Connector host
80	HTTP	Provides HTTP access from client web browsers to the local user interface
443	HTTPS	Provides HTTPS access from client web browsers to the local user interface
TCP	3128	Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deploying the Connector.

Outbound rules

The predefined security group for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for the Connector includes the following outbound rules.

Port	Protocol	Purpose
All	All TCP	All outbound traffic
All	All UDP	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.

ℹ️ The source IP address is the Connector host.

Service	Port	Protocol	Destination	Purpose
API calls and AutoSupport	443	HTTPS	Outbound internet and ONTAP cluster management LIF	API calls to Azure and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp
DNS	53	UDP	DNS	Used for DNS resolve by Cloud Manager

Set up Cloud Volumes ONTAP to use a customer-managed key in Azure

Data is automatically encrypted on Cloud Volumes ONTAP in Azure using Azure Storage Service Encryption with a Microsoft-managed key. But you can use your own encryption key instead by following the steps on this page.

Data encryption overview

Cloud Volumes ONTAP data is automatically encrypted in Azure using Azure Storage Service Encryption. The default implementation uses a Microsoft-managed key. No setup is required.

If you want to use a customer-managed key with Cloud Volumes ONTAP, then you need to complete the following steps:

1. From Azure, create a key vault and then generate a key in that vault

2. From Cloud Manager, use the API to create a Cloud Volumes ONTAP working environment that uses the key

Key rotation

If you create a new version of your key, Cloud Volumes ONTAP automatically uses the latest key version.

How data is encrypted

After you create a Cloud Volumes ONTAP working environment that is configured to use a customer-managed key, Cloud Volumes ONTAP data is encrypted as follows.

HA pairs
  • All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key.

- Any new storage accounts (for example, when you add disks or aggregates) also use the same key.

Single node

- All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key.
- For root, boot, and data disks, Cloud Manager uses a disk encryption set, which enables management of encryption keys with managed disks.
- Any new data disks also use the same disk encryption set.
- NVRAM and the core disk are encrypted using a Microsoft-managed key, instead of the customer-managed key.

Create a key vault and generate a key

The key vault must reside in the same Azure subscription and region in which you plan to create the Cloud Volumes ONTAP system.

Steps

1. Create a key vault in your Azure subscription.

   Note the following requirements for the key vault:

   - The key vault must reside in the same region as the Cloud Volumes ONTAP system.
   - The following options should be enabled:
     - **Soft-delete** (this option is enabled by default, but must *not* be disabled)
     - **Purge protection**
     - **Azure Disk Encryption for volume encryption** (for single node Cloud Volumes ONTAP systems only)

2. Generate a key in the key vault.

   Note the following requirements for the key:

   - The key type must be **RSA**.
   - The recommended RSA key size is **2048**, but other sizes are supported.

Create a working environment that uses the encryption key

After you create the key vault and generate an encryption key, you can create a new Cloud Volumes ONTAP system that is configured to use the key. These steps are supported by using the Cloud Manager API.

Required permissions

If you want to use a customer-managed key with a single node Cloud Volumes ONTAP system, ensure that the Cloud Manager Connector has the following permissions:

```
"Microsoft.Compute/diskEncryptionSets/read"
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write"
```

View the latest list of permissions

ⓘ | The first three permissions aren't required for HA pairs.

Steps

1. Obtain the list of key vaults in your Azure subscription by using the following Cloud Manager API call.

   For an HA pair: `GET /azure/ha/metadata/vaults`

   For single node: `GET /azure/vsa/metadata/vaults`

   Make note of the **name** and **resourceGroup**. You'll need to specify those values in the next step.

   Learn more about this API call.

2. Obtain the list of keys within the vault by using the following Cloud Manager API call.

   For an HA pair: `GET /azure/ha/metadata/keys-vault`

   For single node: `GET /azure/vsa/metadata/keys-vault`

   Make note of the **keyName**. You'll need to specify that value (along with the vault name) in the next step.

   Learn more about this API call.

3. Create a Cloud Volumes ONTAP system by using the following Cloud Manager API call.
   a. For an HA pair:

      `POST /azure/ha/working-environments`

      The request body must include the following fields:

      ```
      "azureEncryptionParameters": {
              "key": "keyName",
              "vaultName": "vaultName"
      }
      ```

      Learn more about this API call.

   b. For a single node system:

```
POST /azure/vsa/working-environments
```

The request body must include the following fields:

```
"azureEncryptionParameters": {
        "key": "keyName",
        "vaultName": "vaultName"
}
```

Learn more about this API call.

Result

You have a new Cloud Volumes ONTAP system that is configured to use your customer-managed key for data encryption.

Set up licensing for Cloud Volumes ONTAP in Azure

After you decide which licensing option you want to use with Cloud Volumes ONTAP, a few steps are required before you can choose that licensing option when creating a new working environment.

Freemium

Select the Freemium offering to use Cloud Volumes ONTAP free of charge with up to 500 GiB of provisioned capacity. Learn more about the Freemium offering.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.

   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Azure Marketplace.

   You won't be charged through the marketplace subscription unless you exceed 500 GiB of provisioned capacity, at which time the system is automatically converted to the Essentials package.

b. After you return to Cloud Manager, select **Freemium** when you reach the charging methods page.

View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.

Capacity-based license

Capacity-based licensing enables you to pay for Cloud Volumes ONTAP per TiB of capacity. Capacity-based licensing is available in the form of a *package*: the Essentials package or the Professional package.

The Essentials and Professional packages are available with the following consumption models:

- A license (BYOL) purchased from NetApp

- An hourly, pay-as-you-go (PAYGO) subscription from the Azure Marketplace

- An annual contract

Learn more about capacity-based licensing.

The following sections describe how to get started with each of these consumption models.

BYOL

Pay upfront by purchasing a license (BYOL) from NetApp to deploy Cloud Volumes ONTAP systems in any cloud provider.

Steps

1. Contact NetApp Sales to obtain a license

2. Add your NetApp Support Site account to Cloud Manager

   Cloud Manager automatically queries NetApp's licensing service to obtain details about the licenses associated with your NetApp Support Site account. If there are no errors, Cloud Manager automatically adds the licenses to the Digital Wallet.

   Your license must be available from the Digital Wallet before you can use it with Cloud Volumes ONTAP. If needed, you can manually add the license to the Digital Wallet.

3. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.

   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Azure Marketplace.

   The license that you purchased from NetApp is always charged first, but you'll be charged from the hourly rate in the marketplace if you exceed your licensed capacity or if the term of your license expires.

b. After you return to Cloud Manager, select a capacity-based package when you reach the charging methods page.

View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.

PAYGO subscription

Pay hourly by subscribing to the offer from your cloud provider's marketplace.

When you create a Cloud Volumes ONTAP working environment, Cloud Manager prompts you to subscribe to the agreement that's available in the Azure Marketplace. That subscription is then associated with the working

environment for charging. You can use that same subscription for additional working environments.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.

   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Azure Marketplace.

   b. After you return to Cloud Manager, select a capacity-based package when you reach the charging methods page.

View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.

> 💡 You can manage the Azure Marketplace subscriptions associated with your Azure accounts from the Settings > Credentials page. Learn how to manage your Azure accounts and subscriptions

Annual contract

Pay for Cloud Volumes ONTAP annually by purchasing an annual contract.

Steps

1. Contact your NetApp sales representative to purchase an annual contract.

   The contract is available as a *private* offer in the Azure Marketplace.

   After NetApp shares the private offer with you, you can select the annual plan when you subscribe from the Azure Marketplace during working environment creation.

2. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.

   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription > Continue**.

   b. In the Azure portal, select the annual plan that was shared with your Azure account and then click **Subscribe**.

   c. After you return to Cloud Manager, select a capacity-based package when you reach the charging methods page.

View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.

Keystone Flex Subscription

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service. Learn more about Keystone Flex Subscriptions.

Steps

1. If you don't have a subscription yet, contact NetApp

2. Contact NetApp to authorize your Cloud Manager user account with one or more Keystone Flex

Subscriptions.

3. After NetApp authorizes your account, link your subscriptions for use with Cloud Volumes ONTAP.

4. On the Canvas page, click **Add Working Environment** and follow the steps in Cloud Manager.

   a. Select the Keystone Flex Subscription charging method when prompted to choose a charging method.

View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.

Enable high availability mode in Azure

Microsoft Azure's high availability mode should be enabled to reduce unplanned failover times and to enable NFSv4 support for Cloud Volumes ONTAP.

Starting with the Cloud Volumes ONTAP 9.10.1 release, we reduced the unplanned failover time for Cloud Volumes ONTAP HA pairs running in Microsoft Azure and added support for NFSv4. To make these enhancements available to Cloud Volumes ONTAP, you need to enable the high availability feature on your Azure subscription.

Cloud Manager will prompt you with these details in an Action Required message when the feature needs to be enabled on an Azure subscription.

Note the following:

- There are no problems with the high availability of your Cloud Volumes ONTAP HA pair. This Azure feature works in concert with ONTAP to reduce the client observed application outage time for NFS protocols that result from unplanned failover events.

- Enabling this feature is non-disruptive to Cloud Volumes ONTAP HA pairs.

- Enabling this feature on your Azure subscription won't cause issues to other VMs.

An Azure user who has "Owner" privileges can enable the feature from the Azure CLI.

Steps

1. [Access the Azure Cloud Shell from the Azure Portal](#)

2. Register the high availability mode feature:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Optionally verify that the feature is now registered:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

The Azure CLI should return a result similar to the following:

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Launching Cloud Volumes ONTAP in Azure

You can launch a single node system or an HA pair in Azure by creating a Cloud Volumes ONTAP working environment in Cloud Manager.

What you'll need

You need the following to create a working environment.

- A Connector that's up and running.
  - You should have a [Connector that is associated with your workspace](#).
  - [You should be prepared to leave the Connector running at all times](#).

- An understanding of the configuration that you want to use.

  You should have chose a configuration and obtained Azure networking information from your administrator. For details, see Planning your Cloud Volumes ONTAP configuration.

- An understanding of what's required to set up licensing for Cloud Volumes ONTAP.

  Learn how to set up licensing.

About this task

When Cloud Manager creates a Cloud Volumes ONTAP system in Azure, it creates several Azure objects, such as a resource group, network interfaces, and storage accounts. You can review a summary of the resources at the end of the wizard.

> **Potential for Data Loss**
>
> The best practice is to use a new, dedicated resource group for each Cloud Volumes ONTAP system.
>
> Deploying Cloud Volumes ONTAP in an existing, shared resource group is not recommended due to the risk of data loss. While Cloud Manager can remove Cloud Volumes ONTAP resources from a shared resource group in case of deployment failure or deletion, an Azure user might accidentally delete Cloud Volumes ONTAP resources from a shared resource group.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the prompts.

2. **Choose a Location**: Select **Microsoft Azure** and **Cloud Volumes ONTAP Single Node** or **Cloud Volumes ONTAP High Availability**.

3. If you're prompted, create a Connector.

4. **Details and Credentials**: Optionally change the Azure credentials and subscription, specify a cluster name, add tags if needed, and then specify credentials.

   The following table describes fields for which you might need guidance:

Field	Description
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the Azure virtual machine. It also uses the name as the prefix for the predefined security group, if you select that option.
Resource Group Tags	Tags are metadata for your Azure resources. When you enter tags in this field, Cloud Manager adds them to the resource group associated with the Cloud Volumes ONTAP system. You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment. For information about tags, refer to Microsoft Azure Documentation: Using tags to organize your Azure resources.

Field	Description
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Credentials	You can choose different Azure credentials and a different Azure subscription to use with this Cloud Volumes ONTAP system. You need to associate an Azure Marketplace subscription with the selected Azure subscription in order to deploy a pay-as-you-go Cloud Volumes ONTAP system. Learn how to add credentials.

The following video shows how to associate a Marketplace subscription to an Azure subscription:

► https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-

ontap//media/video_subscribing_azure.mp4 *(video)*

5. **Services**: Keep the services enabled or disable the individual services that you don't want to use with Cloud Volumes ONTAP.

   ◦ Learn more about Cloud Data Sense.
   ◦ Learn more about Cloud Backup.
   ◦ Learn more about the Monitoring service.

6. **Location**: Select a region, availability zone, VNet, and subnet, and then select the checkbox to confirm network connectivity between the Connector and the target location.

   For single node systems, you can choose the Availability Zone in which you'd like to deploy Cloud Volumes ONTAP. If you don't select an AZ, Cloud Manager will select one for you.

7. **Connectivity**: Choose a new or existing resource group and then choose whether to use the predefined security group or to use your own.

   The following table describes fields for which you might need guidance:

Field	Description
Availability Zone	For single node systems, you can choose the Availability Zone in which you'd like to deploy Cloud Volumes ONTAP. If you don't select an AZ, Cloud Manager will select one for you.
Resource Group	Create a new resource group for Cloud Volumes ONTAP or use an existing resource group. The best practice is to use a new, dedicated resource group for Cloud Volumes ONTAP. While it is possible to deploy Cloud Volumes ONTAP in an existing, shared resource group, it's not recommended due to the risk of data loss. See the warning above for more details. You must use a dedicated resource group for each Cloud Volumes ONTAP HA pair that you deploy in Azure. Only one HA pair is supported in a resource group. Cloud Manager experiences connection issues if you try to deploy a second Cloud Volumes ONTAP HA pair in an Azure resource group. If the Azure account that you're using has the required permissions, Cloud Manager removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.
Generated security group	If you let Cloud Manager generate the security group for you, you need to choose how you'll allow traffic: • If you choose **Selected VNet only**, the source for inbound traffic is the subnet range of the selected VNet and the subnet range of the VNet where the Connector resides. This is the recommended option. • If you choose **All VNets**, the source for inbound traffic is the 0.0.0.0/0 IP range.
Use existing	If you choose an existing security group, then it must meet Cloud Volumes ONTAP requirements. View the default security group.

8. **Charging Methods and NSS Account**: Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.

    ◦ Learn about licensing options for Cloud Volumes ONTAP.

    ◦ Learn how to set up licensing.

9. **Preconfigured Packages**: Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

    If you choose one of the packages, you only need to specify a volume and then review and approve the configuration.

10. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select a virtual machine type.

    ⓘ   If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

11. **Subscribe from the Azure Marketplace**: Follow the steps if Cloud Manager could not enable programmatic deployments of Cloud Volumes ONTAP.

12. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type, a size for each disk, and whether data tiering to Blob storage should be enabled.

    Note the following:

    ◦ The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.

    ◦ The disk size is for all disks in the initial aggregate and for any additional aggregates that Cloud Manager creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

      For help choosing a disk type and size, see Sizing your system in Azure.

    ◦ You can choose a specific volume tiering policy when you create or edit a volume.

    ◦ If you disable data tiering, you can enable it on subsequent aggregates.

      Learn more about data tiering.

13. **Write Speed & WORM** (single node systems only): Choose **Normal** or **High** write speed, and activate write once, read many (WORM) storage, if desired.

    Learn more about write speed.

    WORM can't be enabled if data tiering was enabled.

    Learn more about WORM storage.

14. **Secure Communication to Storage & WORM** (HA only): Choose whether to enable an HTTPS connection to Azure storage accounts, and activate write once, read many (WORM) storage, if desired.

    The HTTPS connection is from a Cloud Volumes ONTAP 9.7 HA pair to Azure storage accounts. Note that enabling this option can impact write performance. You can't change the setting after you create the working environment.

[Learn more about WORM storage](#).

15. **Create Volume**: Enter details for the new volume or click **Skip**.

    [Learn about supported client protocols and versions](#).

    Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.
Initiator group and IQN (for iSCSI only)	iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs. iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs). When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

The following image shows the Volume page filled out for the CIFS protocol:

Volume Details, Protection & Protocol

Details & Protection

Volume Name: | Size (GB):
vol | 250

Snapshot Policy:
default
ⓘ Default Policy

Protocol

NFS | CIFS | iSCSI

Share name: | Permissions:
vol_share | Full Control

Users / Groups:
engineering
Valid users and groups separated by a semicolon

16. **CIFS Setup**: If you chose the CIFS protocol, set up a CIFS server.

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter **OU=AADDC Computers** or **OU=AADDC Users** in this field. Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager automation docs for details. Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

17. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency

features and change the volume tiering policy, if needed.

For more information, see Understanding volume usage profiles and Data tiering overview.

18. **Review & Approve**: Review and confirm your selections.

    a. Review details about the configuration.

    b. Click **More information** to review details about support and the Azure resources that Cloud Manager will purchase.

    c. Select the **I understand…** check boxes.

    d. Click **Go**.

Result

Cloud Manager deploys the Cloud Volumes ONTAP system. You can track the progress in the timeline.

If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the working environment and click **Re-create environment**.

For additional help, go to NetApp Cloud Volumes ONTAP Support.

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

- If you want to apply quotas to volumes, use System Manager or the CLI.

  Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

Use Cloud Volumes ONTAP

License management

Manage capacity-based licenses

Manage your capacity-based licenses from the Digital Wallet to ensure that your NetApp account has enough capacity for your Cloud Volumes ONTAP systems.

Capacity-based licenses enable you to pay for Cloud Volumes ONTAP per TiB of capacity.

The *Digital Wallet* enables you to manage licenses for Cloud Volumes ONTAP from a single location. You can add new licenses and update existing licenses.

Learn more about Cloud Volumes ONTAP licenses.

How licenses are added to the Digital Wallet

After you purchase a license from your NetApp sales representative, NetApp will send you an email with the serial number and additional licensing details.

In the meantime, Cloud Manager automatically queries NetApp's licensing service to obtain details about the licenses associated with your NetApp Support Site account. If there are no errors, Cloud Manager automatically adds the licenses to the Digital Wallet.

If Cloud Manager can't add the license, you'll need to manually add them to the Digital Wallet yourself. For example, if the Connector is installed in a location that doesn't have internet access, you'll need to add the licenses yourself. Learn how to add purchased licenses to your account.

View the consumed capacity in your account

The Digital Wallet shows you the total consumed capacity in your account and the consumed capacity by licensing package. This can help you understand how you're being charged and whether you need to purchase additional capacity.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. With **Capacity Based Licenses** selected, view the packages summary, which shows you consumed capacity, total licensed capacity, and total PAYGO capacity.

   ◦ *Total consumed capacity* is the total provisioned capacity of all Cloud Volumes ONTAP systems in your NetApp account. The charging is based on each volume's provisioned size, regardless of local, used, stored, or effective space within the volume.

   ◦ *Total licensed* is the total licensed capacity (BYOL) that you purchased from NetApp.

   ◦ *Total PAYGO* is the total provisioned capacity using cloud marketplace subscriptions. Charging via PAYGO is used only if the consumed capacity is higher than the licensed capacity or if there is no BYOL license available in the Digital Wallet.

   Here's an example of an account that has 2000 TiB of consumed capacity:

3. Under the summary, view the consumed capacity for each of your licensing packages.

    ◦ *Consumed capacity* shows you the total capacity of the volumes for that package. For more details about a specific package, hover your mouse over the tooltip.

      To better understand the capacities that display for the Essentials package, you should be familiar with how charging works. Learn about charging for the Essentials package.

    ◦ *BYOL* shows you the licensed capacity that you purchased from NetApp.

    ◦ *PAYGO* shows you the total consumed capacity by license consumption model.

      Here's an example for an account that has several licensing packages:

Add purchased licenses to your account

If you don't see your purchased licenses in the Digital Wallet, you'll need to add the licenses to Cloud Manager so that the capacity is available for Cloud Volumes ONTAP.

What you'll need

  • You need to provide Cloud Manager the serial number of the license or the license file.

  • If you want to enter the serial number, you first need to add your NetApp Support Site account to Cloud Manager. This is the NetApp Support Site account that's authorized to access the serial number.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. On the **Cloud Volumes ONTAP** tab, keep **Capacity Based Licenses** selected and click **Add License**.

3. Enter the serial number for your capacity-based license or upload the license file.

   If you entered a serial number, you also need to select the NetApp Support Site account that's authorized to access the serial number.

4. Click **Add License**.

Update a capacity-based license

If you purchased additional capacity or extended the term of your license, Cloud Manager automatically updates the license in the Digital Wallet. There's nothing that you need to do.

However, if you deployed Cloud Manager in a location that doesn't have internet access, then you'll need to manually update the license in Cloud Manager.

What you'll need

The license file (or *files* if you have an HA pair).

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, click the action menu next to the license and select **Update License**.
3. Upload the license file.
4. Click **Upload License**.

Change charging methods

You can change the charging method for a Cloud Volumes ONTAP system that uses capacity-based licensing. For example, if you deployed a Cloud Volumes ONTAP system with the Essentials package, you can change it to the Professional package if your business needs changed.

Limitation

Changing to or from the Edge Cache license isn't supported.

Important note

If you have a private offer or contract from your cloud provider's marketplace, changing to a charging method that's not included in your contract will result in charging against BYOL (if you purchased a license from NetApp) or PAYGO.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, click **Change Charging Method**.
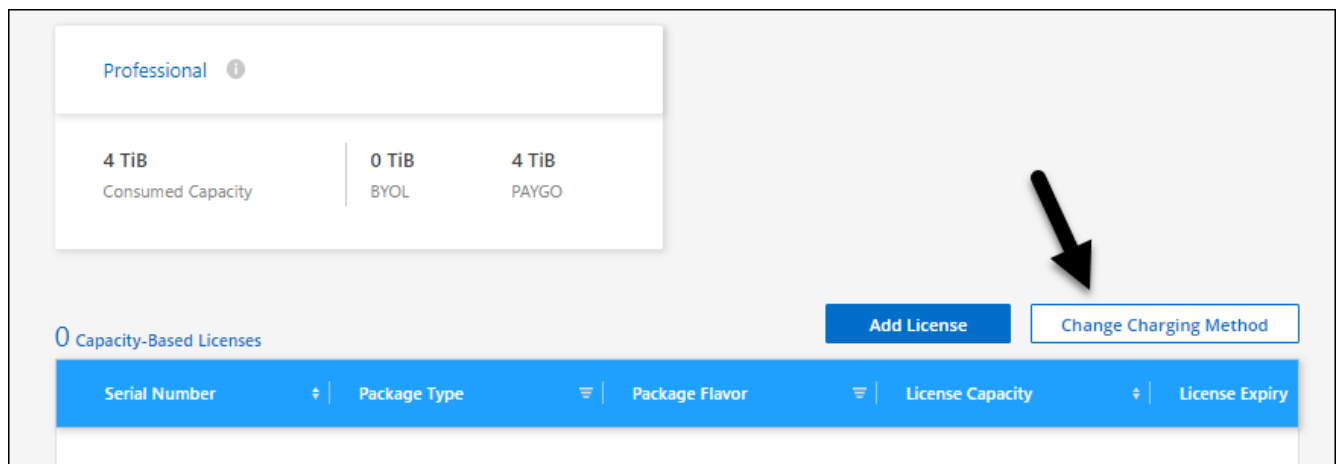
3. Select a working environment, choose the new charging method, and then confirm your understanding that changing the package type will affect service charges.

4. Click **Change Charging Method**.

Result

Cloud Manager changes the charging method for the Cloud Volumes ONTAP system.

You might also notice that the Digital Wallet refreshes the consumed capacity for each package type to account for the change that you just made.

Remove a capacity-based license

If a capacity-based license expired and is no longer in use, then you can remove it at any time.

Steps
1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, click the action menu next to the license and select **Remove License**.
3. Click **Remove** to confirm.

Manage Keystone Flex Subscriptions

Manage your Keystone Flex Subscriptions from the Digital Wallet by enabling subscriptions for use with Cloud Volumes ONTAP. You can also request changes to the committed capacity and you can unlink subscriptions.

A *Keystone Flex Subscription* is a pay-as-you-grow storage service offered by NetApp.

The *Digital Wallet* enables you to manage licenses for Cloud Volumes ONTAP from a single location. You can add new licenses and update existing licenses.

Learn more about Cloud Volumes ONTAP licenses.

Authorize your account

Before you can use and manage Keystone Flex Subscriptions in Cloud Manager, you need to contact NetApp to authorize your Cloud Manager user account with your Keystone Flex Subscriptions.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. Click **Keystone Flex Subscription**.

3. If you see the **Welcome to NetApp Keystone** page, send an email to the address listed on the page.

   A NetApp representative will process your request by authorizing your user account to access the subscriptions.

4. Come back to the **Keystone Flex Subscription** to view your subscriptions.

What's next?

Link the subscriptions that you want to use with Cloud Volumes ONTAP.

Link a subscription

After NetApp authorizes your account, you need to link Keystone Flex Subscriptions for use with Cloud Volumes ONTAP. This action enables users to select the subscription as the charging method for new Cloud Volumes ONTAP systems.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. Click **Keystone Flex Subscription**.

3. For the subscription that you want to link, click ••• and select **Link**.

Result

The subscription is now linked to your Cloud Manager account and available to select when creating a Cloud Volumes ONTAP working environment.

Request more or less committed capacity

If you need to adjust the committed capacity for a subscription, you can send a request right from the Cloud Manager interface.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. Click **Keystone Flex Subscription**.
3. For the subscription that you want adjust the capacity, click ••• and select **View detail and edit**.
4. Enter the requested committed capacity for one or more subscriptions.

5. Scroll down, enter any additional details for the request, and then click **Submit**.

Result

Your request creates a ticket in NetApp's system for processing.

Unlink a subscription

If you no longer want to use a Keystone Flex Subscription with new Cloud Volumes ONTAP systems, you can unlink the subscription. Note that you can only unlink a subscription that isn't attached to an existing Cloud Volumes ONTAP subscription.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. Click **Keystone Flex Subscription**.

3. For the subscription that you want to unlink, click ••• and select **Unlink**.

Result

The subscription is unlinked from your Cloud Manager account and no longer available to select when creating a Cloud Volumes ONTAP working environment.

Manage node-based licenses

Manage node-based licenses in the Digital Wallet to ensure that each Cloud Volumes ONTAP system has a valid license with the required capacity.

Node-based licenses are the previous generation licensing model (and not available for new customers):

- BYOL licenses purchased from NetApp
- Hourly pay-as-you-go (PAYGO) subscriptions from your cloud provider's marketplace

The *Digital Wallet* enables you to manage licenses for Cloud Volumes ONTAP from a single location. You can add new licenses and update existing licenses.

Learn more about Cloud Volumes ONTAP licenses.

Manage PAYGO licenses

The Digital Wallet page enables you to view details about each of your PAYGO Cloud Volumes ONTAP systems, including the serial number and PAYGO license type.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. Click **PAYGO**.
4. View details in the table about each of your PAYGO licenses.
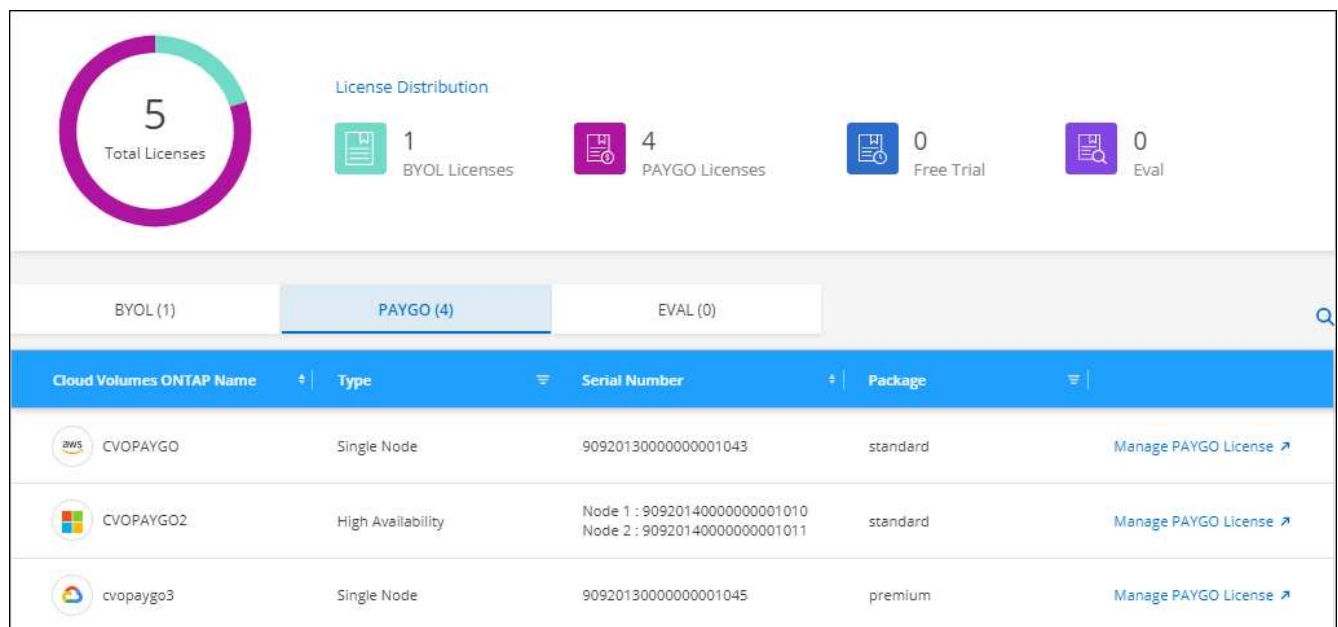
5. If needed, click **Manage PAYGO License** to change the PAYGO license or to change the instance type.

Manage BYOL licenses

Manage licenses that you purchased directly from NetApp by adding and removing system licenses and extra capacity licenses.

Add unassigned licenses

Add a node-based license to the Digital Wallet so that you can select the license when you create a new Cloud Volumes ONTAP system. The Digital Wallet identifies these licenses as *unassigned*.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.

3. Click **Unassigned**.

4. Click **Add Unassigned Licenses**.

5. Enter the serial number of the license or upload the license file.

   If you don't have the license file yet, refer to the section below.

6. Click **Add License**.

Result

Cloud Manager adds the license to the Digital Wallet. The license will be identified as unassigned until you associate it with a new Cloud Volumes ONTAP system. After that happens, the license moves to the **BYOL** tab in the Digital Wallet.

Exchange unassigned node-based licenses

If you have an unassigned node-based license for Cloud Volumes ONTAP that you haven't used, you can exchange the license by converting it to a Cloud Backup license, a Cloud Data Sense license, or a Cloud Tiering license.

Exchanging the license revokes the Cloud Volumes ONTAP license and creates a dollar-equivalent license for the service:

- Licensing for a Cloud Volumes ONTAP HA pair is converted to a 51 TiB data service license
- Licensing for a Cloud Volumes ONTAP single node is converted to a 32 TiB data service license

The converted license has the same expiry date as the Cloud Volumes ONTAP license.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.

3. Click **Unassigned**.

4. Click **Exchange License**.

5. Select the service that you'd like to exchange the license with.

6. If you're prompted, select an additional license for the HA pair.

7. Read the legal consent and click **Agree**.

Result

Cloud Manager converts the unassigned license to the service that you selected. You can view the new license in the **Data Services Licenses** tab.

Obtain a system license file

In most cases, Cloud Manager can automatically obtain your license file using your NetApp Support Site account. But if it can't, then you'll need to manually upload the license file. If you don't have the license file, you can obtain it from netapp.com.

Steps

1. Go to the NetApp License File Generator and log in using your NetApp Support Site credentials.

2. Enter your password, choose your product, enter the serial number, confirm that you have read and accepted the privacy policy, and then click **Submit**.

   Example

3. Choose whether you want to receive the serialnumber.NLF JSON file through email or direct download.

Update a system license

When you renew a BYOL subscription by contacting a NetApp representative, Cloud Manager automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system.

If Cloud Manager can't access the license file over the secure internet connection, you can obtain the file yourself and then manually upload the file to Cloud Manager.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.

3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.

4. Click the action menu next to the system license and select **Update License**.

5. Upload the license file (or files if you have an HA pair).

6. Click **Update License**.

Result

Cloud Manager updates the license on the Cloud Volumes ONTAP system.

Manage extra capacity licenses

You can purchase extra capacity licenses for a Cloud Volumes ONTAP BYOL system to allocate more than the 368 TiB of capacity that's provided with a BYOL system license. For example, you might purchase one extra license capacity to allocate up to 736 TiB of capacity to Cloud Volumes ONTAP. Or you could purchase three extra capacity licenses to get up to 1.4 PiB.

The number of licenses that you can purchase for a single node system or HA pair is unlimited.

Add capacity licenses

Purchase an extra capacity license by contacting us through the chat icon in the lower-right of Cloud Manager. After you purchase the license, you can apply it to a Cloud Volumes ONTAP system.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
4. Click **Add Capacity License**.
5. Enter the serial number or upload the license file (or files if you have an HA pair).
6. Click **Add Capacity License**.

Update capacity licenses

If you extended the term of an extra capacity license, you'll need to update the license in Cloud Manager.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
4. Click the action menu next to the capacity license and select **Update License**.
5. Upload the license file (or files if you have an HA pair).
6. Click **Update License**.

Remove capacity licenses

If an extra capacity license expired and is no longer in use, then you can remove it at any time.

Steps

1. From the left navigation menu, select **Digital Wallet**.
2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.
3. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.

4. Click the action menu next to the capacity license and select **Remove License**.

5. Click **Remove**.

Convert an Eval license to a BYOL

An evaluation license is good for 30 days. You can apply a new BYOL license on top of the evaluation license for an in-place upgrade.

When you convert an Eval license to a BYOL, Cloud Manager restarts the Cloud Volumes ONTAP system.

- For a single-node system, the restart results in I/O interruption during the reboot process.
- For an HA pair, the restart initiates takeover and giveback to continue serving I/O to clients.

Steps

1. From the left navigation menu, select **Digital Wallet**.

2. On the **Cloud Volumes ONTAP** tab, select **Node Based Licenses** from the drop-down.

3. Click **Eval**.

4. In the table, click **Convert to BYOL License** for a Cloud Volumes ONTAP system.

5. Enter the serial number or upload the license file.

6. Click **Convert License**.

Result

Cloud Manager starts the conversion process. Cloud Volumes ONTAP automatically restarts as part of this process. When it's back up, the licensing information will reflect the new license.

Change between PAYGO and BYOL

Converting a system from PAYGO by-node licensing to BYOL by-node licensing (and vice versa) isn't supported. If you want to switch between a pay-as-you-go subscription and a BYOL subscription, then you need to deploy a new system and replicate data from the existing system to the new system.

Steps

1. Create a new Cloud Volumes ONTAP working environment.

2. Set up a one-time data replication between the systems for each volume that you need to replicate.

   Learn how to replicate data between systems

3. Terminate the Cloud Volumes ONTAP system that you no longer need by deleting the original working environment.

   Learn how to delete a Cloud Volumes ONTAP working environment.

Volume and LUN administration

Create FlexVol volumes

If you need more storage after you launch your initial Cloud Volumes ONTAP system, you can create new FlexVol volumes for NFS, CIFS, or iSCSI from Cloud Manager.

Cloud Manager provides several ways to create a new volume:

- Specify details for a new volume and let Cloud Manager handle the underlying data aggregates for you. Learn more.

- Create a volume on a data aggregate of your choice. Learn more.

- Create volume from a template to optimize the volume for the workload requirements for certain applications, such as databases or streaming services. Learn more.

- Create a volume on the second node in an HA configuration. Learn more.

Before you get started

A few notes about volume provisioning:

- When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

- You can create additional LUNs from System Manager or the CLI.

Create a volume

The most common way to create a volume is to specify the type of volume that you need and then Cloud Manager handles the disk allocation for you. But you also have the option to choose the specific aggregate on which you want to create the volume.

Steps

1. On the Canvas page, double-click the name of the Cloud Volumes ONTAP system on which you want to provision a FlexVol volume.

2. Create a new volume by letting Cloud Manager handle the disk allocation for you, or choose a specific aggregate for the volume.

   Choosing a specific aggregate is recommended only if you have a good understanding of the data aggregates on your Cloud Volumes ONTAP system.

   > **Any aggregate**
   > In the Volumes tab, click **Add Volume** > **New volume**.
   >
   > **Specific aggregate**
   > a. Click the menu icon, and then click **Advanced > Advanced allocation**.
   > b. Click the menu for an aggregate.
   > c. Click **Create volume**.

3. Follow the steps in the wizard to create the volume.

   a. **Details, Protection, and Tags**: Enter basic details about the volume and select a Snapshot policy.

      Some of the fields on this page are self-explanatory. The following list describes fields for which you might need guidance:

Field	Description
Volume Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Tags	Tags that you add to a volume are associated with the Application Templates service, which can help you organize and simplify the management of your resources.
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.

b. **Protocol**: Choose a protocol for the volume (NFS, CIFS, or iSCSI) and then provide the required information.

   If you select CIFS and a server isn't set up, Cloud Manager prompts you to set up CIFS connectivity after you click **Next**.

   Learn about supported client protocols and versions.

   The following sections describe fields for which you might need guidance. The descriptions are organized by protocol.

NFS

Access control

Choose a custom export policy to make the volume available to clients.

Export policy

Defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.

CIFS

Permissions and users/groups

Enables you to control the level of access to an SMB share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.

DNS Primary and Secondary IP Address

The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.

Active Directory Domain to join

The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.

Credentials authorized to join the domain

The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.

CIFS server NetBIOS name

A CIFS server name that is unique in the AD domain.

Organizational Unit

The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.

- To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, enter **OU=AADDC Computers** or **OU=AADDC Users** in this field.
  Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain

DNS Domain

The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

NTP Server

Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager automation docs for details.

Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

> **iSCSI**
>
> **LUN**
>
> iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.
>
> **Initiator group**
>
> Initiator groups (igroups) specify which hosts can access specified LUNs on the storage system
>
> **Host initiator (IQN)**
>
> iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs).

c. **Disk Type**: Choose an underlying disk type for the volume based on your performance needs and cost requirements.

   ▪ Sizing your system in Azure

d. **Usage Profile & Tiering Policy**: Choose whether to enable or disable storage efficiency features on the volume and then select a volume tiering policy.

ONTAP includes several storage efficiency features that can reduce the total amount of storage that you need. NetApp storage efficiency features provide the following benefits:

Thin provisioning

Presents more logical storage to hosts or users than you actually have in your physical storage pool. Instead of preallocating storage space, storage space is allocated dynamically to each volume as data is written.

Deduplication

Improves efficiency by locating identical blocks of data and replacing them with references to a single shared block. This technique reduces storage capacity requirements by eliminating redundant blocks of data that reside in the same volume.

Compression

Reduces the physical capacity required to store data by compressing data within a volume on primary, secondary, and archive storage.

e. **Review**: Review details about the volume and then click **Add**.

Result

Cloud Manager creates the volume on the Cloud Volumes ONTAP system.

Create a volume from a template

If your organization has created Cloud Volumes ONTAP volume templates so you can deploy volumes that are optimized for the workload requirements for certain applications, follow the steps in this section.

The template should make your job easier because certain volume parameters will already be defined in the

template, such as disk type, size, protocol, snapshot policy, cloud provider, and more. When a parameter is already predefined, you can just skip to the next volume parameter.

> ⓘ   You can only create NFS or CIFS volumes when using templates.

Steps

1. On the Canvas page, click the name of the Cloud Volumes ONTAP system on which you want to provision a volume.

2.
   Click ⋮ > **Add Volume From Template**.
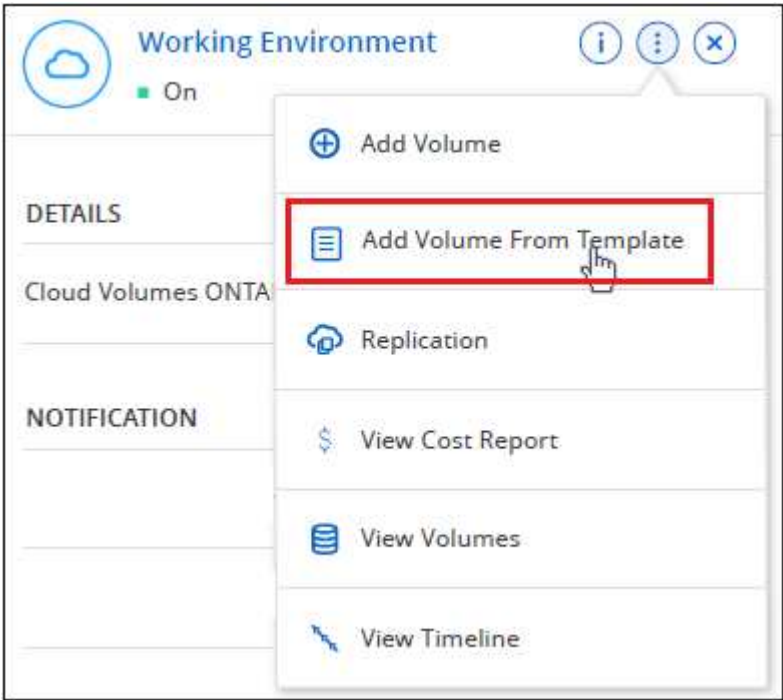
3. In the *Select Template* page, select the template that you want to use to create the volume and click **Next**.

The *Define Parameters* page is displayed.

> ⓘ You can click the checkbox **Show read-only parameters** to show all the fields that have been locked by the template if you want to see the values for those parameters. By default these predefined fields are hidden and only the fields you need to complete are shown.
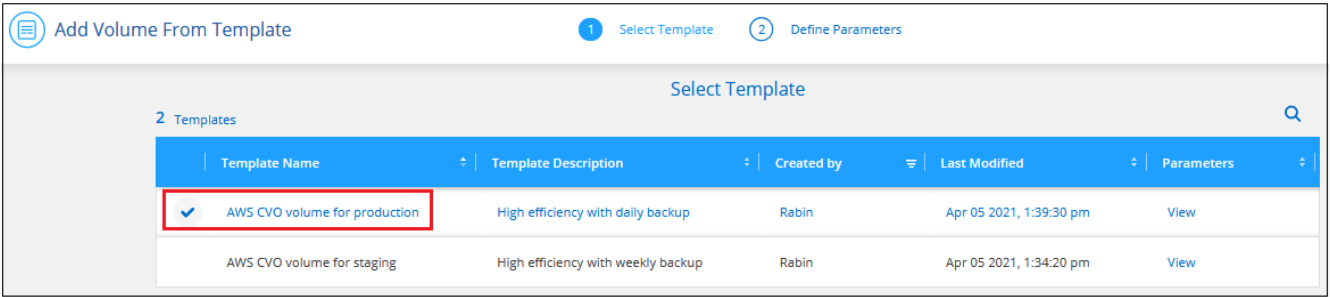
4. In the *Context* area, the Working Environment is filled in with the name of the working environment you started with. You need to select the **Storage VM** where the volume will be created.

5. Add values for all of the parameters that are not hard-coded from the template. See Create a volume for details about all the parameters you need to complete to deploy a Cloud Volumes ONTAP volume.

6. If there are no other Actions that you need to define (for example, configuring Cloud Backup), click **Run Template**.

   If there are other actions, click the action in the left pane to display the parameters you need to complete.

   For example, if the Enable Cloud Backup action requires that you select a backup policy, you can do that now.

7. Click **Run Template**.

Result

Cloud Volumes ONTAP provisions the volume and displays a page so that you can see the progress.

Additionally, if any secondary action is implemented in the template, for example, enabling Cloud Backup on the volume, that action is also performed.

Create a volume on the second node in an HA configuration

By default, Cloud Manager creates volumes on the first node in an HA configuration. If you need an active-active configuration, in which both nodes serve data to clients, you must create aggregates and volumes on the second node.

Steps

1. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment on which you want to manage aggregates.

2. Click the menu icon and then click **Advanced > Advanced allocation**.

3. Click **Add Aggregate** and then create the aggregate.

4. For Home Node, choose the second node in the HA pair.

5. After Cloud Manager creates the aggregate, select it and then click **Create volume**.

6. Enter details for the new volume, and then click **Create**.

Result

Cloud Manager creates the volume on the second node in the HA pair.

After you create a volume

If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

If you want to apply quotas to volumes, you must use System Manager or the CLI. Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

Manage existing volumes

Cloud Manager enables you to manage volumes and CIFS servers. It also prompts you to move volumes to avoid capacity issues.

Manage volumes

You can manage volumes as your storage needs change. You can view, edit, clone, restore, and delete volumes.

Steps

1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.

2. Manage your volumes:

Task	Action
View information about a volume	Select a volume, and then click **Info**.
Edit a volume (read-write volumes only)	a. Select a volume, and then click **Edit**. b. Modify the volume's Snapshot policy, NFS protocol version, NFS access control list (export policy), or share permissions, and then click **Update**. ⓘ If you need custom Snapshot policies, you can create them by using System Manager.
Clone a volume	a. Select a volume, and then click **Clone**. b. Modify the clone name as needed, and then click **Clone**. This process creates a FlexClone volume. A FlexClone volume is a writable, point-in-time copy that is space-efficient because it uses a small amount of space for metadata, and then only consumes additional space as data is changed or added. To learn more about FlexClone volumes, see the ONTAP 9 Logical Storage Management Guide.
Restore data from a Snapshot copy to a new volume	a. Select a volume, and then click **Restore from Snapshot copy**. b. Select a Snapshot copy, enter a name for the new volume, and then click **Restore**.
Create a Snapshot copy on demand	a. Select a volume, and then click **Create a Snapshot copy**. b. Change the name, if needed, and then click **Create**.
Get the NFS mount command	a. Select a volume, and then click **Mount Command**. b. Click **Copy**.

Task	Action
View the target iQN for an iSCSI volume	a. Select a volume, and then click **Target iQN**. b. Click **Copy**. c. Use the IQN to connect to the LUN from your hosts.
Change the underlying disk type	a. Select a volume, and then click **Change Disk Type & Tiering Policy**. b. Select the disk type, and then click **Change**. (i) Cloud Manager moves the volume to an existing aggregate that uses the selected disk type or it creates a new aggregate for the volume.
Change the tiering policy	a. Select a volume, and then click **Change Disk Type & Tiering Policy**. b. Click **Edit Policy**. c. Select a different policy and click **Change**. (i) Cloud Manager moves the volume to an existing aggregate that uses the selected disk type with tiering, or it creates a new aggregate for the volume.
Delete a volume	a. Select a volume, and then click **Delete**. b. Click **Delete** again to confirm.

Resize a volume

By default, a volume automatically grows to a maximum size when it's out of space. The default value is 1,000, which means the volume can grow to 11 times it's size. This value is configurable in a Connector's settings.

If you need to resize your volume, you can do it through ONTAP System Manager. Be sure to take your system's capacity limits into consideration as you resize volumes. Go to the Cloud Volumes ONTAP Release Notes for more details.

Modify the CIFS server

If you change your DNS servers or Active Directory domain, you need to modify the CIFS server in Cloud Volumes ONTAP so that it can continue to serve storage to clients.

Steps
1. From the working environment, click the menu icon and then click **Advanced > CIFS setup**.
2. Specify settings for the CIFS server:

Task	Action
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. • To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, enter **OU=AADDC Computers** or **OU=AADDC Users** in this field. Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.

3. Click **Save**.

Result

Cloud Volumes ONTAP updates the CIFS server with the changes.

Move a volume

Move volumes for capacity utilization, improved performance, and to satisfy service-level agreements.

You can move a volume in System Manager by selecting a volume and the destination aggregate, starting the volume move operation, and optionally monitoring the volume move job. When using System Manager, a volume move operation finishes automatically.

Steps

1. Use System Manager or the CLI to move the volumes to the aggregate.

   In most situations, you can use System Manager to move volumes.

   For instructions, see the ONTAP 9 Volume Move Express Guide.

Move a volume when Cloud Manager displays an Action Required message

Cloud Manager might display an Action Required message that says moving a volume is necessary to avoid capacity issues, but that you need to correct the issue yourself. If this happens, you need to identify how to correct the issue and then move one or more volumes.

Cloud Manager displays these Action Required messages when an aggregate has reached 90% used capacity. If data tiering is enabled, the messages display when an aggregate has reached 80% used capacity. By default, 10% free space is reserved for data tiering. Learn more about the free space ratio for data tiering.

Steps

1. Identify how to correct the issue.

2. Based on your analysis, move volumes to avoid capacity issues:

   ◦ Move volumes to another system.

   ◦ Move volumes to another aggregate on the same system.

Identify how to correct capacity issues

If Cloud Manager can't provide recommendations for moving a volume to avoid capacity issues, you must identify the volumes that you need to move and whether you should move them to another aggregate on the same system or to another system.

Steps

1. View the advanced information in the Action Required message to identify the aggregate that has reached its capacity limit.

   For example, the advanced information should say something similar to the following: Aggregate aggr1 has reached its capacity limit.

2. Identify one or more volumes to move out of the aggregate:

   a. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.

   b. Select the aggregate, and then click **Info**.

   c. Expand the list of volumes.

Used Aggregate Capacity:	105.66 GB
Volumes:	4

   Vol54 (54 GB)

   data_vol (150 GB)

   svm_FinanceOnPrem_root (1 GB)

   d. Review the size of each volume and choose one or more volumes to move out of the aggregate.

   You should choose volumes that are large enough to free space in the aggregate so that you avoid additional capacity issues in the future.

3. If the system has not reached the disk limit, you should move the volumes to an existing aggregate or a new aggregate on the same system.

For details, see Moving volumes to another aggregate to avoid capacity issues.

4. If the system has reached the disk limit, do any of the following:

   a. Delete any unused volumes.

   b. Rearrange volumes to free space on an aggregate.

      For details, see Moving volumes to another aggregate to avoid capacity issues.

   c. Move two or more volumes to another system that has space.

      For details, see Moving volumes to another system to avoid capacity issues.

Move volumes to another system to avoid capacity issues

You can move one or more volumes to another Cloud Volumes ONTAP system to avoid capacity issues. You might need to do this if the system reached its disk limit.

About this task

You can follow the steps in this task to correct the following Action Required message:

```
Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
```

Steps

1. Identify a Cloud Volumes ONTAP system that has available capacity, or deploy a new system.

2. Drag and drop the source working environment on the target working environment to perform a one-time data replication of the volume.

   For details, see Replicating data between systems.

3. Go to the Replication Status page, and then break the SnapMirror relationship to convert the replicated volume from a data protection volume to a read/write volume.

   For details, see Managing data replication schedules and relationships.

4. Configure the volume for data access.

   For information about configuring a destination volume for data access, see the ONTAP 9 Volume Disaster Recovery Express Guide.

5. Delete the original volume.

   For details, see Manage volumes.

Move volumes to another aggregate to avoid capacity issues

You can move one or more volumes to another aggregate to avoid capacity issues.

About this task

You can follow the steps in this task to correct the following Action Required message:

```
Moving two or more volumes is necessary to avoid capacity issues; however,
Cloud Manager cannot perform this action for you.
```

Steps

1. Verify whether an existing aggregate has available capacity for the volumes that you need to move:

   a. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.

   b. Select each aggregate, click **Info**, and then view the available capacity (aggregate capacity minus used aggregate capacity).

   ## aggr1

Aggregate Capacity:	442.94 GB
Used Aggregate Capacity:	105.66 GB

2. If needed, add disks to an existing aggregate:

   a. Select the aggregate, and then click **Add disks**.

   b. Select the number of disks to add, and then click **Add**.

3. If no aggregates have available capacity, create a new aggregate.

   For details, see Creating aggregates.

4. Use System Manager or the CLI to move the volumes to the aggregate.

5. In most situations, you can use System Manager to move volumes.

   For instructions, see the ONTAP 9 Volume Move Express Guide.

Reasons why a volume move might perform slowly

Moving a volume might take longer than you expect if any of the following conditions are true for Cloud Volumes ONTAP:

- The volume is a clone.
- The volume is a parent of a clone.
- The source or destination aggregate has a single Throughput Optimized HDD (st1) disk.
- One of the aggregates uses an older naming scheme for objects. Both aggregates have to use the same name format.

  An older naming scheme is used if data tiering was enabled on an aggregate in the 9.4 release or earlier.

- The encryption settings don't match on the source and destination aggregates, or a rekey is in progress.

- The *-tiering-policy* option was specified on the volume move to change the tiering policy.

- The *-generate-destination-key* option was specified on the volume move.

Tiering inactive data to low-cost object storage

You can reduce storage costs for Cloud Volumes ONTAP by combining an SSD or HDD performance tier for hot data with an object storage capacity tier for inactive data. Data tiering is powered by FabricPool technology. For a high-level overview, see Data tiering overview.

To set up data tiering, you need to do the following:

1   **Choose a supported configuration**

Most configurations are supported. If you have a Cloud Volumes ONTAP system running the most recent version, then you should be good to go. Learn more.

2   **Ensure connectivity between Cloud Volumes ONTAP and object storage**

- For Azure, you won't need to do anything as long as Cloud Manager has the required permissions. Learn more.

3   **Ensure that you have an aggregate with tiering enabled**

Data tiering must be enabled on an aggregate in order to enable data tiering on a volume. You should be aware of the requirements for new volumes and for existing volumes. Learn more.

4   **Choose a tiering policy when creating, modifying, or replicating a volume**

Cloud Manager prompts you to choose a tiering policy when you create, modify, or replicate a volume.

- Tiering data on read-write volumes

- Tiering data on data protection volumes

> **What's not required for data tiering?**
>
> - You don't need to install a feature license to enable data tiering.
>
> - You don't need to create an object store for the capacity tier. Cloud Manager does that for you.
>
> - You don't need to enable data tiering at the system level.
>
>   Cloud Manager creates an object store for cold data when the system is created, as long as there are no connectivity or permissions issues. After that, you just need to enable data tiering on volumes (and in some cases, on aggregates).

Configurations that support data tiering

You can enable data tiering when using specific configurations and features.

Support in Azure

- Data tiering is supported in Azure as follows:
    - Version 9.4 in with single node systems
    - Version 9.6 in with HA pairs
- The performance tier can be Premium SSD managed disks, Standard SSD managed disks, or Standard HDD managed disks.

Feature interoperability

- Data tiering is supported with encryption technologies.
- Thin provisioning must be enabled on volumes.

Requirements

Depending on your cloud provider, certain connections and permissions must be set up so that Cloud Volumes ONTAP can tier cold data to object storage.

Requirements to tier cold data to Azure Blob storage

You don't need to set up a connection between the performance tier and the capacity tier as long as Cloud Manager has the required permissions. Cloud Manager enables a VNet service endpoint for you if the custom role for the Connector has these permissions:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

The permissions are included in the custom role by default. View Azure permission for the Connector

Enabling data tiering after implementing the requirements

Cloud Manager creates an object store for cold data when the system is created, as long as there are no connectivity or permissions issues. If you didn't implement the requirements listed above until after you created the system, then you'll need to manually enable tiering, which creates the object store.

Steps

1. Ensure that you've met all requirements.
2. On the Canvas page, double-click the name of the Cloud Volumes ONTAP instance.
3. Click the menu icon and select **Enable capacity tiering**.

You'll only see this option if data tiering couldn't be enabled when Cloud Manager created the system.

In Google Cloud, a service account must be attached to Cloud Volumes ONTAP before this option will appear. Ensure that you've met all requirements.

4. Click **Enable** so Cloud Manager can create the object store that this Cloud Volumes ONTAP system will use for tiered data.

Ensuring that tiering is enabled on aggregates

Data tiering must be enabled on an aggregate in order to enable data tiering on a volume. You should be aware of the requirements for new volumes and for existing volumes.

- **New volumes**

  If you're enabling data tiering on a new volume, then you don't need to worry about enabling data tiering on an aggregate. Cloud Manager creates the volume on an existing aggregate that has tiering enabled, or it creates a new aggregate for the volume if a data tiering-enabled aggregate doesn't already exist.

- **Existing volumes**

  If you want to enable data tiering on an existing volume, then you'll need to ensure that data tiering is enabled on the underlying aggregate. If data tiering isn't enabled on the existing aggregate, then you'll need to use System Manager to attach an existing aggregate to the object store.

Steps to confirm whether tiering is enabled on an aggregate

1. Open the working environment in Cloud Manager.
2. Click the menu icon, click **Advanced**, and then click **Advanced allocation**.
3. Verify whether tiering is enabled or disabled on the aggregate.

Steps to enable tiering on an aggregate

1. In System Manager, click **Storage > Tiers**.
2. Click the action menu for the aggregate and select **Attach Cloud Tiers**.
3. Select the cloud tier to attach and click **Save**.

What's next?

You can now enable data tiering on new and existing volumes, as explained in the next section.

Tiering data from read-write volumes

Cloud Volumes ONTAP can tier inactive data on read-write volumes to cost-effective object storage, freeing up the performance tier for hot data.

Steps

1. In the working environment, create a new volume or change the tier of an existing volume:

Task	Action
Create a new volume	Click **Add New Volume**.
Modify an existing volume	Select the volume and click **Change Disk Type & Tiering Policy**.

2. Select a tiering policy.

   For a description of these policies, see Data tiering overview.

   Example

Cloud Manager creates a new aggregate for the volume if a data tiering-enabled aggregate does not already exist.

Tiering data from data protection volumes

Cloud Volumes ONTAP can tier data from a data protection volume to a capacity tier. If you activate the destination volume, the data gradually moves to the performance tier as it is read.

Steps

1. On the Canvas page, select the working environment that contains the source volume, and then drag it to the working environment to which you want to replicate the volume.

2. Follow the prompts until you reach the tiering page and enable data tiering to object storage.

   Example

   For help with replicating data, see Replicating data to and from the cloud.

Changing the storage class for tiered data

After you deploy Cloud Volumes ONTAP, you can reduce your storage costs by changing the storage class for inactive data that hasn't been accessed for 30 days. The access costs are higher if you do access the data, so you must take that into consideration before you change the storage class.

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

For information about supported storage classes, see Data tiering overview.

Steps

1. From the working environment, click the menu icon and then click **Storage Classes** or **Blob Storage Tiering**.

2. Choose a storage class and then click **Save**.

Changing the free space ratio for data tiering

The free space ratio for data tiering defines how much free space is required on Cloud Volumes ONTAP SSDs/HDDs when tiering data to object storage. The default setting is 10% free space, but you can tweak the setting based on your requirements.

For example, you might choose less than 10% free space to ensure that you are utilizing the purchased capacity. Cloud Manager can then purchase additional disks for you when additional capacity is required (up until you reach the disk limit for the aggregate).

> ⚠️ If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data and you might experience performance degradation. Any change should be done with caution. If you're unsure, reach out to NetApp support for guidance.

The ratio is important for disaster recovery scenarios because as data is read from the object store, Cloud Volumes ONTAP moves the data to SSDs/HDDs to provide better performance. If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data. Take this into consideration when changing the ratio so that you can meet your business requirements.

Steps

1. In the upper right of the Cloud Manager console, click the **Settings** icon, and select **Connector Settings**.

2. Under **Capacity**, click **Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering**.

3. Change the free space ratio based on your requirements and click **Save**.

Changing the cooling period for the auto tiering policy

If you enabled data tiering on a Cloud Volumes ONTAP volume using the *auto* tiering policy, you can adjust the default cooling period based on your business needs. This action is supported using the API only.

The cooling period is the number of days that user data in a volume must remain inactive before it is considered "cold" and moved to object storage.

The default cooling period for the auto tiering policy is 31 days. You can change the cooling period as follows:

- 9.8 or later: 2 days to 183 days

- 9.7 or earlier: 2 days to 63 days

Step

1. Use the *minimumCoolingDays* parameter with your API request when creating a volume or modifying an existing volume.

Connect a LUN to a host

When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

Note the following:

- Cloud Manager's automatic capacity management doesn't apply to LUNs. When Cloud Manager creates a LUN, it disables the autogrow feature.
- You can create additional LUNs from System Manager or the CLI.

Steps

1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.
2. Select a volume, and then click **Target iQN**.
3. Click **Copy** to copy the iQN name.
4. Set up an iSCSI connection from the host to the LUN.

   - ONTAP 9 iSCSI express configuration for Red Hat Enterprise Linux: Starting the iSCSI sessions with the target
   - ONTAP 9 iSCSI express configuration for Windows: Starting iSCSI sessions with the target
   - ONTAP SAN host configuration

Accelerate data access with FlexCache volumes

A FlexCache volume is a storage volume that caches NFS read data from an origin (or source) volume. Subsequent reads to the cached data result in faster access to that data.

You can use FlexCache volumes to speed up access to data or to offload traffic from heavily accessed volumes. FlexCache volumes help improve performance, especially when clients need to access the same data repeatedly, because the data can be served directly without having to access the origin volume. FlexCache volumes work well for system workloads that are read-intensive.

Cloud Manager does not provide management of FlexCache volumes at this time, but you can use the ONTAP CLI or ONTAP System Manager to create and manage FlexCache volumes:

- FlexCache Volumes for Faster Data Access Power Guide
- Creating FlexCache volumes in System Manager

Starting with the 3.7.2 release, Cloud Manager generates a FlexCache license for all new Cloud Volumes ONTAP systems. The license includes a 500 GiB usage limit.

Aggregate administration

Create aggregates

You can create aggregates yourself or let Cloud Manager do it for you when it creates volumes. The benefit of creating aggregates yourself is that you can choose the underlying disk size, which enables you to size your aggregate for the capacity or the performance that you need.

> ⚠️ 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.

Steps

1. On the Canvas page, double-click the name of the Cloud Volumes ONTAP instance on which you want to manage aggregates.

2. Click the menu icon, and then click **Advanced > Advanced allocation**.

3. Click **Add Aggregate** and then specify details for the aggregate.

   > **Azure**
   >
   > For help with disk type and disk size, refer to Plan your Cloud Volumes ONTAP configuration in Azure.

4. Click **Go**, and then click **Approve and Purchase**.

Manage aggregates

Manage aggregates yourself by adding disks, viewing information about the aggregates, and by deleting them.

> ⚠️ 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.

Before you begin

If you want to delete an aggregate, you must have first deleted the volumes in the aggregate.

About this task

If an aggregate is running out of space, you can move volumes to another aggregate by using System Manager.

Steps

1. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
2. Click the menu icon and then click **Advanced > Advanced allocation**.
3. Manage your aggregates:

Task	Action
View information about an aggregate	Select an aggregate and click **Info**.
Create a volume on a specific aggregate	Select an aggregate and click **Create volume**.
Add disks to an aggregate	a. Select an aggregate and click **Add disks**. b. Select the number of disks that you want to add and click **Add**. 💡 All disks in an aggregate must be the same size.
Delete an aggregate	a. Select an aggregate that does not contain any volumes and click **Delete**. b. Click **Delete** again to confirm.

Manage capacity settings on a Connector

Each Connector has settings that determines how it manages aggregate capacity for Cloud Volumes ONTAP.

These settings affect all Cloud Volumes ONTAP systems managed by a Connector. If you have another Connector, it can be configured differently.

Required permissions

Account Admin privileges are required to modify Connector settings.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.

2. Under **Capacity**, modify any of the following settings:

    Capacity Management Mode

    Choose whether Cloud Manager notifies you of storage capacity decisions or whether Cloud Manager automatically manages capacity requirements for you.

    Learn how Capacity Management Mode works.

    Free Space Ratio

    Triggers a notification when the free space ratio on an aggregate drops below the specified threshold.

    The free space ratio is calculated as follows:

    (aggregate capacity - total used capacity on the aggregate) / aggregate capacity

    Free Space Ratio for Data Tiering

    Defines how much free space is required on the performance tier (disks) when tiering data to a capacity tier (object storage).

    The ratio is important for disaster recovery scenarios. As data is read from the capacity tier, Cloud Volumes ONTAP moves data to the performance tier to provide better performance. If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data.

3. Click **Save**.

Storage VM administration

Manage storage VMs in Cloud Manager

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but some configurations support additional storage VMs.

Supported number of storage VMs

Multiple storage VMs are supported with certain configurations. Go to the Cloud Volumes ONTAP Release Notes to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

Work with multiple storage VMs

Cloud Manager supports any additional storage VMs that you create from System Manager or the CLI.

For example, the following image shows how you can choose a storage VM when you create a volume.

And the following image shows how you can choose a storage VM when replicating a volume to another system.

Modify the name of the default storage VM

Cloud Manager automatically names the single storage VM that it creates for Cloud Volumes ONTAP. You can modify the name of the storage VM if you have strict naming standards. For example, you might want the name to match how you name the storage VMs for your ONTAP clusters.

If you created any additional storage VMs for Cloud Volumes ONTAP, then you can't rename the storage VMs from Cloud Manager. You'll need to do so directly from Cloud Volumes ONTAP by using System Manager or

the CLI.

Steps

1. From the working environment, click the menu icon, and then click **Information**.

2. Click the edit icon to the right of the storage VM name.

3. In the Modify SVM Name dialog box, change the name, and then click **Save**.

Manage storage VMs for disaster recovery

Cloud Manager doesn't provide any setup or orchestration support for storage VM disaster recovery. You must use System Manager or the CLI.

- SVM Disaster Recovery Preparation Express Guide
- SVM Disaster Recovery Express Guide

Create data-serving storage VMs for Cloud Volumes ONTAP in Azure

A storage VM is a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*. Cloud Volumes ONTAP is configured with one storage VM by default, but additional storage VMs are supported when running Cloud Volumes ONTAP in Azure.

To create additional data-serving storage VMs, you need to allocate IP addresses in Azure and then run ONTAP commands to create the storage VM and data LIFs.

Supported number of storage VMs

Multiple storage VMs are supported with specific Cloud Volumes ONTAP configurations starting with the 9.9.0 release. Go to the Cloud Volumes ONTAP Release Notes to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All other Cloud Volumes ONTAP configurations support one data-serving storage VM and one destination storage VM used for disaster recovery. You can activate the destination storage VM for data access if there's an outage on the source storage VM.

Allocate IP addresses in Azure

You need to allocate IP addresses in Azure before you create a storage VM and allocate LIFs.

Single node system

IP addresses must be assigned to nic0 in Azure before you create a storage VM and allocate LIFs.

You'll need to create an IP address for data LIF access and another optional IP address for a storage VM (SVM) management LIF. This management LIF provides a connection to management tools like SnapCenter.

Steps
1. Log in to the Azure portal and open the **Virtual machine** service.
2. Click the name of the Cloud Volumes ONTAP VM.
3. Click **Networking**.
4. Click the name of the network interface for nic0.
5. Under **Settings**, click **IP configurations**.
6. Click **Add**.
7. Enter a name for the IP configuration, select **Dynamic**, and then click **OK**.
8. Click the name of the IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

   It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

If you want to create an SVM management LIF, repeat these steps to create an additional IP address.

After you finish

Copy the private IP addresses that you just created. You'll need to specify those IP addresses when you create LIFs for the new storage VM.

HA pair

How you allocate IP addresses for an HA pair depends on the storage protocol that you're using.

iSCSI

iSCSI IP addresses must be assigned to nic0 in Azure before you create a storage VM and allocate LIFs. IPs for iSCSI are assigned to nic0 and not the load balancer because iSCSI uses ALUA for failover.

You'll need to create the following IP addresses:

- One IP address for iSCSI data LIF access from node 1

- One IP address for iSCSI data LIF access from node 2

- An optional IP address for a storage VM (SVM) management LIF

  This management LIF provides a connection to management tools like SnapCenter.

Steps

1. Log in to the Azure portal and open the **Virtual machine** service.

2. Click the name of the Cloud Volumes ONTAP VM for node 1.

3. Click **Networking**.

4. Click the name of the network interface for nic0.

5. Under **Settings**, click **IP configurations**.

6. Click **Add**.

7. Enter a name for the IP configuration, select **Dynamic**, and then click **OK**.

8. Click the name of the IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

   It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

9. Repeat these steps on node 2.

10. If you want to create an SVM management LIF, repeat these steps on node 1.

NFS

IP addresses that you use for NFS are allocated in the load balancer so that the IP addresses can migrate to the other node in case failover events occur.

You'll need to create the following IP addresses:

- One IP address for NAS data LIF access from node 1

- One IP address for NAS data LIF access from node 2

- An optional IP address for a storage VM (SVM) management LIF

  This management LIF provides a connection to management tools like SnapCenter.

Steps

1. In the Azure portal, open the **Load balancers** service.

2. Click the name of the load balancer for the HA pair.

3. Create one frontend IP configuration for data LIF access from node 1, another for data LIF access from node 2, and another optional frontend IP for a storage VM (SVM) management LIF.

a. Under **Settings**, click **Frontend IP configuration**.

b. Click **Add**.

c. Enter a name for the frontend IP, select the subnet for the Cloud Volumes ONTAP HA pair, leave **Dynamic** selected, and in regions with Availability Zones, leave **Zone-redundant** selected to ensure that the IP address remains available if a zone fails.

d. Click the name of the frontend IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

   It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

4. Add a health probe for each frontend IP that you just created.

   a. Under the load balancer's **Settings**, click **Health probes**.

   b. Click **Add**.

   c. Enter a name for the health probe and enter a port number that's between 63005 and 65000. Keep the default values for the other fields.

      It's important that the port number is between 63005 and 65000. For example, if you are creating three health probes, you could enter probes that use the port numbers 63005, 63006, and 63007.

5. Create new load balancing rules for each frontend IP.

   a. Under the load balancer's **Settings**, click **Load balancing rules**.

   b. Click **Add** and enter the required information:

      - **Name**: Enter a name for the rule.

      - **IP Version**: Select **IPv4**.

      - **Frontend IP address**: Select one of the frontend IP addresses that you just created.

      - **HA Ports**: Enable this option.

      - **Backend pool**: Keep the default Backend pool that was already selected.

      - **Health probe**: Select the health probe that you created for the selected frontend IP.

      - **Session persistence**: Select **None**.

      - **Floating IP**: Select **Enabled**.

Add load balancing rule ⋯
chandanaTcpRst3-rg-lb

ℹ A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *

jimmy_new_rule ✓

IP Version *

⦿ IPv4 ◯ IPv6

Frontend IP address * ℹ

10.1.0.156 (dataAFIP) ⌄

☑ HA Ports ℹ

Backend pool ℹ

backendPool (2 virtual machines) ⌄

Health probe ℹ

dataAProbe (TCP:63002) ⌄

Session persistence ℹ

None ⌄

Floating IP ℹ

(Disabled **Enabled**)

---

6. Ensure that the network security group rules for Cloud Volumes ONTAP allows the load balancer to send TCP probes for the health probes that were created in step 4 above. Note that this is allowed by default.

SMB

IP addresses that you use for SMB data are allocated in the load balancer so that the IP addresses can migrate to the other node in case failover events occur.

You'll need to create the following IP addresses:

- One IP address for NAS data LIF access from node 1
- One IP address for NAS data LIF access from node 2
- One IP address for an iSCSI LIF on node 1
- One IP address for an iSCSI LIF on node 2
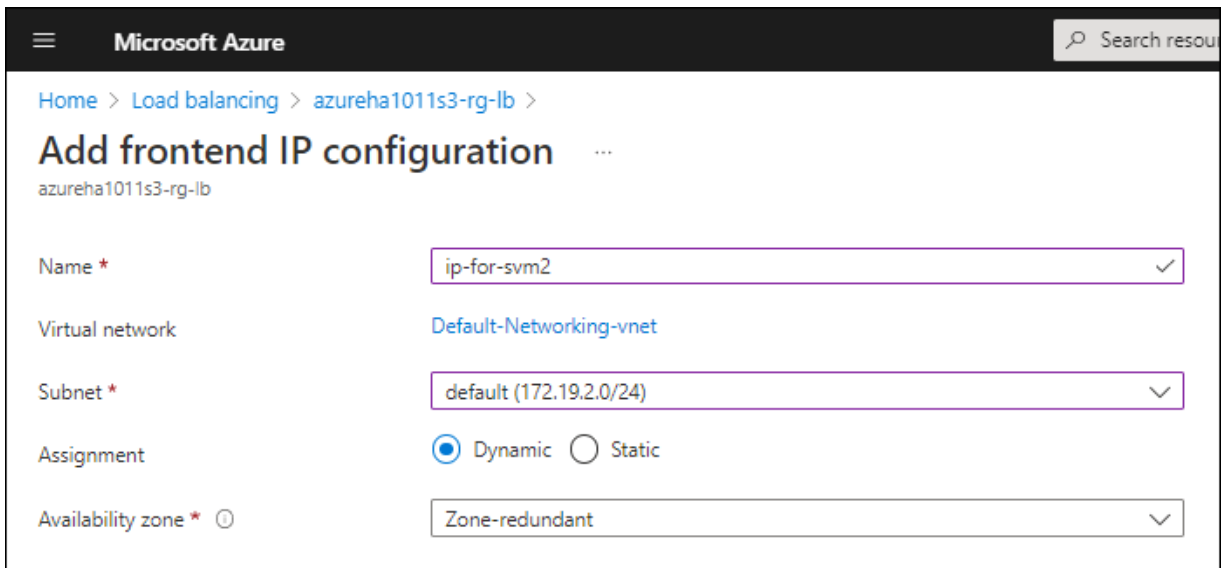
  The iSCSI LIFs are required for DNS and SMB communication. An iSCSI LIF is used for this purpose because it doesn't migrate on failover.

- An optional IP address for a storage VM (SVM) management LIF

  This management LIF provides a connection to management tools like SnapCenter.

Steps

1. In the Azure portal, open the **Load balancers** service.

2. Click the name of the load balancer for the HA pair.

3. Create the required number of frontend IP configurations:

    a. Under **Settings**, click **Frontend IP configuration**.

    b. Click **Add**.

    c. Enter a name for the frontend IP, select the subnet for the Cloud Volumes ONTAP HA pair, leave **Dynamic** selected, and in regions with Availability Zones, leave **Zone-redundant** selected to ensure that the IP address remains available if a zone fails.

    d. Click the name of the frontend IP configuration that you just created, change the **Assignment** to **Static**, and click **Save**.

    It's best to use a static IP address because a static IP ensures that the IP address won't change, which can help to prevent unnecessary outages to your application.

4. Add a health probe for each frontend IP that you just created.

    a. Under the load balancer's **Settings**, click **Health probes**.

    b. Click **Add**.

    c. Enter a name for the health probe and enter a port number that's between 63005 and 65000. Keep the default values for the other fields.

    It's important that the port number is between 63005 and 65000. For example, if you are creating three health probes, you could enter probes that use the port numbers 63005, 63006, and 63007.

5. Create new load balancing rules for each frontend IP.

    a. Under the load balancer's **Settings**, click **Load balancing rules**.

    b. Click **Add** and enter the required information:

- **Name**: Enter a name for the rule.

- **IP Version**: Select **IPv4**.

- **Frontend IP address**: Select one of the frontend IP addresses that you just created.

- **HA Ports**: Enable this option.

- **Backend pool**: Keep the default Backend pool that was already selected.

- **Health probe**: Select the health probe that you created for the selected frontend IP.

- **Session persistence**: Select **None**.

- **Floating IP**: Select **Enabled**.

6. Ensure that the network security group rules for Cloud Volumes ONTAP allows the load balancer to send TCP probes for the health probes that were created in step 4 above. Note that this is allowed by default.

After you finish

Copy the private IP addresses that you just created. You'll need to specify those IP addresses when you create LIFs for the new storage VM.

Create a storage VM and LIFs

After you allocate IP addresses in Azure, you can create a new storage VM on a single node system or on an HA pair.

Single node system

How you create a storage VM and LIFs on a single node system depends on the storage protocol that you're using.

iSCSI

Follow these steps to create a new storage VM, along with the required LIFs.

Steps

1. Create the storage VM and a route to the storage VM.

   ```
   vserver create -vserver <svm-name> -subtype default -rootvolume
   <root-volume-name> -rootvolume-security-style unix
   ```

   ```
   network route create -destination 0.0.0.0/0 -vserver <svm-name>
   -gateway <ip-of-gateway-server>
   ```

2. Create a data LIF:

   ```
   network interface create -vserver <svm-name> -home-port e0a -address
   <iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data
   -protocol iscsi
   ```

3. Optional: Create a storage VM management LIF.

   ```
   network interface create -vserver <svm-name> -lif <lif-name> -role
   data -data-protocol none -address <svm-mgmt-ip-address> -netmask
   -length <length> -home-node <name-of-node1> -status-admin up
   -failover-policy system-defined -firewall-policy mgmt -home-port e0a
   -auto-revert false -failover-group Default
   ```

4. Assign one or more aggregates to the storage VM.

   ```
   vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
   ```

   This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

NFS

Follow these steps to create a new storage VM, along with the required LIFs.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. Create a data LIF:

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nfs--ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. Optional: Create a storage VM management LIF.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

SMB

Follow these steps to create a new storage VM, along with the required LIFs.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. Create a data LIF:

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nfs--ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. Optional: Create a storage VM management LIF.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

HA pair

How you create a storage VM and LIFs on an HA pair depends on the storage protocol that you're using.

iSCSI

Follow these steps to create a new storage VM, along with the required LIFs.

Steps

1. Create the storage VM and a route to the storage VM.

   ```
   vserver create -vserver <svm-name> -subtype default -rootvolume
   <root-volume-name> -rootvolume-security-style unix
   ```

   ```
   network route create -destination 0.0.0.0/0 -vserver <svm-name>
   -gateway <ip-of-gateway-server>
   ```

2. Create data LIFs:

   a. Use the following command to create an iSCSI LIF on node 1.

      ```
      network interface create -vserver <svm-name> -home-port e0a
      -address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-
      node1> -data-protocol iscsi
      ```

   b. Use the following command to create an iSCSI LIF on node 2.

      ```
      network interface create -vserver <svm-name> -home-port e0a
      -address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-
      node2> -data-protocol iscsi
      ```

3. Optional: Create a storage VM management LIF on node 1.

   ```
   network interface create -vserver <svm-name> -lif <lif-name> -role
   data -data-protocol none -address <svm-mgmt-ip-address> -netmask
   -length <length> -home-node <name-of-node1> -status-admin up
   -failover-policy system-defined -firewall-policy mgmt -home-port e0a
   -auto-revert false -failover-group Default
   ```

   This management LIF provides a connection to management tools like SnapCenter.

4. Assign one or more aggregates to the storage VM.

   ```
   vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
   ```

   This step is required because the new storage VM needs access to at least one aggregate before you

can create volumes on the storage VM.

5. If you're running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

NFS

Follow these steps to create a new storage VM, along with the required LIFs.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. Create data LIFs:

   a. Use the following command to create a NAS LIF on node 1.

   ```
   network interface create -vserver <svm-name> -lif <lif-name>
   -role data -data-protocol cifs,nfs -address <nfs--ip-address>
   -netmask-length <length> -home-node <name-of-node1> -status-admin
   up -failover-policy system-defined -firewall-policy data -home
   -port e0a -auto-revert true -failover-group Default -probe-port
   <port-number-for-azure-health-probe1>
   ```

   b. Use the following command to create a NAS LIF on node 2.

   ```
   network interface create -vserver <svm-name> -lif <lif-name>
   -role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
   -netmask-length <length> -home-node <name-of-node2> -status-admin
   up -failover-policy system-defined -firewall-policy data -home
   -port e0a -auto-revert true -failover-group Default -probe-port
   <port-number-for-azure-health-probe2>
   ```

3. Optional: Create a storage VM management LIF on node 1.

   ```
   network interface create -vserver <svm-name> -lif <lif-name> -role
   data -data-protocol none -address <svm-mgmt-ip-address> -netmask
   -length <length> -home-node <name-of-node1> -status-admin up
   -failover-policy system-defined -firewall-policy mgmt -home-port e0a
   -auto-revert false -failover-group Default -probe-port <port-number-
   for-azure-health-probe3>
   ```

   This management LIF provides a connection to management tools like SnapCenter.

4. Assign one or more aggregates to the storage VM.

   ```
   vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
   ```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

5. If you're running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

SMB

Follow these steps to create a new storage VM, along with the required LIFs.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. Create NAS data LIFs:

   a. Use the following command to create a NAS LIF on node 1.

   ```
   network interface create -vserver <svm-name> -lif <lif-name>
   -role data -data-protocol cifs,nfs -address <nfs--ip-address>
   -netmask-length <length> -home-node <name-of-node1> -status-admin
   up -failover-policy system-defined -firewall-policy data -home
   -port e0a -auto-revert true -failover-group Default -probe-port
   <port-number-for-azure-health-probe1>
   ```

   b. Use the following command to create a NAS LIF on node 2.

   ```
   network interface create -vserver <svm-name> -lif <lif-name>
   -role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
   -netmask-length <length> -home-node <name-of-node2> -status-admin
   up -failover-policy system-defined -firewall-policy data -home
   -port e0a -auto-revert true -failover-group Default -probe-port
   <port-number-for-azure-health-probe2>
   ```

3. Create iSCSI LIFs to provide DNS and SMB communication:

   a. Use the following command to create an iSCSI LIF on node 1.

   ```
   network interface create -vserver <svm-name> -home-port e0a
   -address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-
   node1> -data-protocol iscsi
   ```

   b. Use the following command to create an iSCSI LIF on node 2.

   ```
   network interface create -vserver <svm-name> -home-port e0a
   -address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-
   node2> -data-protocol iscsi
   ```

4. Optional: Create a storage VM management LIF on node 1.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

This management LIF provides a connection to management tools like SnapCenter.

5. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

6. If you're running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

What's next?

After you create a storage VM on an HA pair, it's best to wait 12 hours before you provision storage on that SVM. Starting with the Cloud Volumes ONTAP 9.10.1 release, Cloud Manager scans the settings for an HA pair's load balancer at a 12-hour interval. If there are new SVMs, Cloud Manager will enable a setting that provides shorter unplanned failover.

Security and data encryption

Encrypting volumes with NetApp encryption solutions

Cloud Volumes ONTAP supports NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE). NVE and NAE are software-based solutions that enable FIPS 140-2–compliant data-at-rest encryption of volumes. Learn more about these

[encryption solutions](#).

Both NVE and NAE are supported with an external key manager.

If you use NVE, you have the option to use your cloud provider's key vault to protect ONTAP encryption keys:

- Azure Key Vault (AKV)

New aggregates will have NAE enabled by default after you set up an external key manager. New volumes that aren't part of an NAE aggregate will have NVE enabled by default (for example, if you have existing aggregates that were created before setting up an external key manager).

Cloud Volumes ONTAP doesn't support onboard key management.

What you'll need

Your Cloud Volumes ONTAP system should be registered with NetApp support. A NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support.

- [Adding NetApp Support Site accounts to Cloud Manager](#)
- [Registering pay-as-you-go systems](#)

> ⓘ   Cloud Manager doesn't install the NVE license on systems that reside in the China region.

Steps

1. Review the list of supported key managers in the [NetApp Interoperability Matrix Tool](#).

   > 💡   Search for the **Key Managers** solution.

2. [Connect to the Cloud Volumes ONTAP CLI](#).
3. Configure external key management.
   - Azure: [Azure Key Vault (AKV)](#)

Manage keys with Azure Key Vault

You can use [Azure Key Vault (AKV)](#) to protect your ONTAP encryption keys in an Azure-deployed application.

AKV can be used to protect [NetApp Volume Encryption (NVE) keys](#) only for data SVMs.

Key management with AKV can be enabled with the CLI or the ONTAP REST API.

When using AKV, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (login.microsoftonline.com). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

Prerequisites

- Cloud Volumes ONTAP must be running version 9.10.1 or later
- Volume Encryption (VE) license installed (NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support)
- Multi-tenant Encryption Key Management (MTEKM) license installed

- You must be a cluster or SVM administrator

- An Active Azure subscription

Limitations

- AKV can only be configured on a data SVM

Configuration process

The outlined steps capture how to register your Cloud Volumes ONTAP configuration with Azure and how to create an Azure Key Vault and keys. If you have already completed these steps, ensure you have the correct configuration settings, particularly in Create an Azure Key Vault, and then proceed to Cloud Volumes ONTAP configuration.

- Azure Application Registration

- Create Azure client secret

- Create an Azure Key Vault

- Create encryption key

- Create an Azure Active Directory Endpoint (HA only)

- Cloud Volumes ONTAP configuration

Azure Application Registration

1. You must first register your application in the Azure subscription that you want the Cloud Volumes ONTAP to use for access the Azure Key Vault. Within the Azure portal, select **App registrations**.

2. Select **New registration**.

3. Provide a name for your application and select a supported application type. The default single tenant suffices for Azure Key Vault usage. Select **Register**.

4. In the Azure Overview window, select the application you have registered. Copy the **application (client) ID** and the **directory (tenant) ID** to a secure location. They will be required later in the registration process.

Create Azure client secret

1. In the Azure portal for your Cloud Volumes ONTAP application, select the **Ceritificates & secrets** pane.

2. Select **New client secret** Enter a meaningful name for your client secret. NetApp recommends a 24-month expiration period, however your specific cloud governance policies may require a different setting.

3. Select **Add** to save the client secret. Immediately copy the **Value** of the secret and store it somewhere secure for future configuration. The secret value will not be displayed after you navigate away from the page.

Create an Azure Key Vault

1. If you have an existing Azure Key Vault, you can connect it to your Cloud Volumes ONTAP configuration, however you must adapt the access policies to the settings in this process.

2. In the Azure portal, navigate to the **Key Vaults** section.

3. Select **Create**. Enter the required information including resource group, region and pricing tier and make selections for the days to retain deleted vaults and whether or not purge protection is enabled. For the purposes of this configuration, defaults are sufficient, however your specific cloud governance policies may require different settings.

4. Select **Next** to choose an access policy.

5. Select **Azure Disk Encryption** for the volume encryption option and **Vault access policy** for the permission model.

6. Select **Add Access Policy**.

7. Select the caret adjacent to the **Configure from template (optional)** field. Then, select **Key, Secret, & Certification Management.**

8. Choose each of the drop-down permissions menus (key, secret, certificate) and then **Select all** at the top of the menu list to select all the permissions available. You should have:

   ◦ **Key permissions**: 19 selected

   ◦ **Secret permissions**: 8 selected

   ◦ **Certificate permissions**: 16 selected

9. Select **Add** to create the access policy.

10. Select **Next** to advance to **Networking** options.

11. Choose the appropriate network access method or select **All networks** and **Review + Create** to create the key vault. (Network access method may be prescribed by a governance policy or your corporate cloud security team.)

12. Record the Key Vault URI: In the key vault you created, navigate to the Overview menu and copy the **Vault URI** from the right-hand column. You will need this for a later step.

Create encryption key

1. In the menu for the Key Vault you have created for Cloud Volumes ONTAP, navigate to the **Keys** option.

2. Select **Generate/import** to create a new key.

3. Leave the default option set to **Generate**.

4. Provide the following information:

   ◦ Encryption key name

   ◦ Key type: RSA

   ◦ RSA key size: 2048

   ◦ Enabled: Yes

5. Select **Create** to create the encryption key.

6. Return to the **Keys** menu and select the key you just created.

7. Select the key ID under **Current version** to view the key properties.

8. Locate the **Key Identifier** field. Copy the URI up to but not including the hexadecimal string.

Create an Azure Active Directory Endpoint (HA only)

1. This process is only required if you are configuring Azure Key Vault for an HA Cloud Volumes ONTAP Working Environment.

2. In the Azure portal navigate to **Virtual Networks**.

3. Select the Virtual Network where you deployed the Cloud Volumes ONTAP working environment and select the **Subnets** menu on the left side of the page.

4. Select the subnet name for you Cloud Volumes ONTAP deployment from the list.

5. Navigate to the **Service Endpoints** heading. In the dropdown menu, select **Microsoft.AzureActiveDirectory** from the list.

6. Select **Save** to capture your settings.

Cloud Volumes ONTAP configuration

1. Connect to the cluster management LIF with your preferred SSH client.

2. Enter the advanced privilege mode in ONTAP:
   ```
   set advanced -con off`
   ```

3. Identify the desired data SVM and verify its DNS configuration:
   ```
   vserver services name-service dns show
   ```

   a. If a DNS entry for the desired data SVM exists and it contains an entry for the Azure DNS, then no action is required. If it does not, add a DNS server entry for the data SVM that points to the Azure DNS, private DNS, or on-premise server. This should match the entry for the cluster admin SVM:
   ```
   vserver services name-service dns create -vserver SVM_name -domains domain
   -name-servers IP_address
   ```

   b. Verify the DNS service has been created for the data SVM:
   ```
   vserver services name-service dns show
   ```

4. Enable Azure Key Vault using the client ID and tenant ID saved after the application registration:
   ```
   security key-manager external azure enable -vserver SVM_name -client-id
   Azure_client_ID -tenant-id Azure_tenant_ID -name Azure_key_name -key-id
   Azure_key_ID
   ```

5. Verify the key manager configuration:
   ```
   security key-manager external azure show
   ```

6. Check the status of the key manager:
   ```
   security key-manager external azure check
   ```
   The output will look like:

   ```
   ::*> security key-manager external azure check

   Vserver: data_svm_name
   Node: akvlab01-01

   Category: service_reachability
       Status: OK

   Category: ekmip_server
       Status: OK

   Category: kms_wrapped_key_status
       Status: UNKNOWN
       Details: No volumes created yet for the vserver. Wrapped KEK status
   will be available after creating encrypted volumes.

   3 entries were displayed.
   ```

   If the `service_reachability` status is not `OK`, the SVM cannot reach the Azure Key Vault service with all the required connectivity and permissions.
   The `kms_wrapped_key_status` will report `UNKNOWN` at initial configuration. Its status will change to `OK` after the first volume is encrypted.

7. OPTIONAL: Create a test volume to verify the functionality of NVE.

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
-state online -policy default
```

If configured correctly, Cloud Volumes ONTAP will automatically create the volume and enable volume encryption.

8. Confirm the volume was created and encrypted correctly. If it is, the `-is-encrypted` parameter will display as `true`.

```
vol show -vserver SVM_name -fields is-encrypted
```

Improving protection against ransomware

Ransomware attacks can cost a business time, resources, and reputation. Cloud Manager enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

Using this feature to improve protection against ransomware addresses a separate use case from the ONTAP anti-ransomware feature that you can enable through System Manager or the ONTAP CLI.

Steps

1. From the working environment, click the **Ransomware** icon.
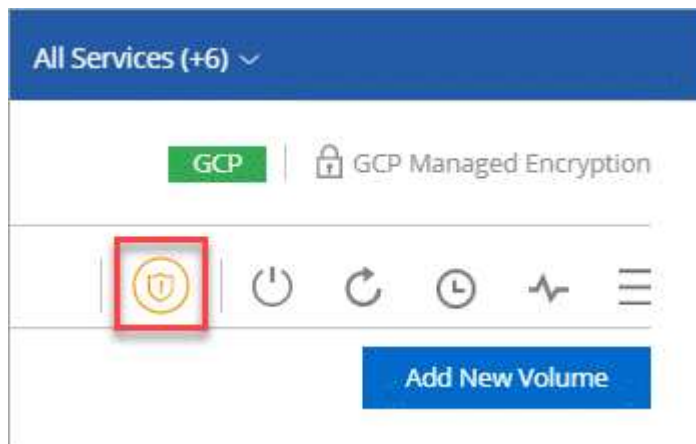
2. Implement the NetApp solution for ransomware:

   a. Click **Activate Snapshot Policy**, if you have volumes that do not have a Snapshot policy enabled.

      NetApp Snapshot technology provides the industry's best solution for ransomware remediation. The key to a successful recovery is restoring from uninfected backups. Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

   b. Click **Activate FPolicy** to enable ONTAP's FPolicy solution, which can block file operations based on a file's extension.

      This preventative solution improves protection from ransomware attacks by blocking common ransomware file types.

      The default FPolicy scope blocks files that have the following extensions:

micro, encrypted, locked, crypto, crypt, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, good, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre

> 💡 Cloud Manager creates this scope when you activate FPolicy on Cloud Volumes ONTAP. The list is based on common ransomware file types. You can customize the blocked file extensions by using the *vserver fpolicy policy scope* commands from the Cloud Volumes ONTAP CLI.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. Learn More

1 Enable Snapshot Copy Protection ⓘ

50 %
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes ⓘ

Activate Snapshot Policy

2 Block Ransomware File Extensions ⓘ

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names ⓘ

Activate FPolicy

System administration

Upgrade Cloud Volumes ONTAP software

Upgrade Cloud Volumes ONTAP from Cloud Manager to gain access to the latest new features and enhancements. You should prepare Cloud Volumes ONTAP systems before you upgrade the software.

Upgrade overview

You should be aware of the following before you start the Cloud Volumes ONTAP upgrade process.

Upgrade from Cloud Manager only

Upgrades of Cloud Volumes ONTAP must be completed from Cloud Manager. You should not upgrade Cloud Volumes ONTAP by using System Manager or the CLI. Doing so can impact system stability.

How to upgrade

Cloud Manager provides two ways to upgrade Cloud Volumes ONTAP:

- By following upgrade notifications that appear in the working environment
- By placing the upgrade image at an HTTPS location and then providing Cloud Manager with the URL

Supported upgrade paths

The version of Cloud Volumes ONTAP that you can upgrade to depends on the version of Cloud Volumes ONTAP that you're currently running.

Current version	Versions that you can directly upgrade to
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Note the following:

- The supported upgrade paths for Cloud Volumes ONTAP are different than they are for an on-premises ONTAP cluster.
- If you upgrade by following the upgrade notifications that appear in a working environment, Cloud Manager will prompt you to upgrade to a release that follows these supported upgrade paths.
- If you upgrade by placing an upgrade image at an HTTPS location, be sure to follow these supported upgrade paths.
- In some cases, you might need to upgrade a few times to reach your target release.

  For example, if you're running version 9.8 and you want to upgrade to 9.10.1, you first need to upgrade to version 9.9.1 and then to 9.10.1.

Reverting or downgrading

Reverting or downgrading Cloud Volumes ONTAP to a previous release is not supported.

Support registration

Cloud Volumes ONTAP must be registered with NetApp support in order to upgrade the software using any of the methods described on this page. This applies to both PAYGO and BYOL. You'll need to manually register PAYGO systems, while BYOL systems are registered by default.

> A system that isn't registered for support will still receive the software update notifications that appear in Cloud Manager when a new version is available. But you will need to register the system before you can upgrade the software.

Upgrades of the HA mediator

Cloud Manager also updates the mediator instance as needed during the Cloud Volumes ONTAP upgrade process.

Prepare to upgrade

Before performing an upgrade, you must verify that your systems are ready and make any required configuration changes.

- Plan for downtime
- Verify that automatic giveback is still enabled
- Suspend SnapMirror transfers
- Verify that aggregates are online

Plan for downtime

When you upgrade a single-node system, the upgrade process takes the system offline for up to 25 minutes, during which I/O is interrupted.

Upgrading an HA pair is nondisruptive and I/O is uninterrupted. During this nondisruptive upgrade process, each node is upgraded in tandem to continue serving I/O to clients.

Verify that automatic giveback is still enabled

Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

ONTAP 9 Documentation: Commands for configuring automatic giveback

Suspend SnapMirror transfers

If a Cloud Volumes ONTAP system has active SnapMirror relationships, it is best to suspend transfers before you update the Cloud Volumes ONTAP software. Suspending the transfers prevents SnapMirror failures. You must suspend the transfers from the destination system.

> Even though Cloud Backup uses an implementation of SnapMirror to create backup files (called SnapMirror Cloud), backups do not need to be suspended when a system is upgraded.

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. Log in to System Manager from the destination system.

   You can log in to System Manager by pointing your web browser to the IP address of the cluster management LIF. You can find the IP address in the Cloud Volumes ONTAP working environment.

   > ⓘ The computer from which you are accessing Cloud Manager must have a network connection to Cloud Volumes ONTAP. For example, you might need to log in to Cloud Manager from a jump host that's in your cloud provider network.

2. Click **Protection > Relationships**.

3. Select the relationship and click **Operations > Quiesce**.

Verify that aggregates are online

Aggregates for Cloud Volumes ONTAP must be online before you update the software. Aggregates should be online in most configurations, but if they are not, then you should bring them online.

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.

2. Select an aggregate, click **Info**, and then verify that the state is online.

   aggr1

Aggregate Capacity:	88.57 GB
Used Aggregate Capacity:	1.07 GB
Volumes:	2 ⌄
AWS Disks:	1 ⌄
State:	online

3. If the aggregate is offline, use System Manager to bring the aggregate online:

   a. Click **Storage > Aggregates & Disks > Aggregates**.

   b. Select the aggregate, and then click **More Actions > Status > Online**.

Upgrade Cloud Volumes ONTAP

Cloud Manager notifies you when a new version is available for upgrade. You can start the upgrade process

from this notification. For details, see Upgrade from Cloud Manager notifications.

Another way to perform software upgrades by using an image on an external URL. This option is helpful if Cloud Manager can't access the S3 bucket to upgrade the software or if you were provided with a patch. For details, see Upgrade from an image available at a URL.

Upgrade from Cloud Manager notifications

Cloud Manager displays a notification in Cloud Volumes ONTAP working environments when a new version of Cloud Volumes ONTAP is available:

You can start the upgrade process from this notification, which automates the process by obtaining the software image from an S3 bucket, installing the image, and then restarting the system.

Before you begin

Cloud Manager operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.

Steps

1. From the left navigation menu, select **Canvas**.

2. Select a working environment.

   A notification appears in the right pane if a new version is available:

3. If a new version is available, click **Upgrade**.

4. In the Release Information page, click the link to read the Release Notes for the specified version, and then select the **I have read…** check box.

5. In the End User License Agreement (EULA) page, read the EULA, and then select **I read and approve the EULA**.

6. In the Review and Approve page, read the important notes, select **I understand…**, and then click **Go**.

Result

Cloud Manager starts the software upgrade. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

Upgrade from an image available at a URL

You can place the Cloud Volumes ONTAP software image on the Connector or on an HTTP server and then initiate the software upgrade from Cloud Manager. You might use this option if Cloud Manager can't access the S3 bucket to upgrade the software.

Before you begin

- Cloud Manager operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.

- If you use HTTPS to host ONTAP images, the upgrade can fail due to SSL authentication issues, which are caused by missing certificates. The workaround is to generate and install a CA-signed certificate to be used for authentication between ONTAP and Cloud Manager.

  Go to the NetApp Knowledge Base to view step-by-step instructions:

Steps

1. Optional: Set up an HTTP server that can host the Cloud Volumes ONTAP software image.

   If you have a VPN connection to the virtual network, you can place the Cloud Volumes ONTAP software image on an HTTP server in your own network. Otherwise, you must place the file on an HTTP server in the cloud.

2. If you use your own security group for Cloud Volumes ONTAP, ensure that the outbound rules allow HTTP connections so Cloud Volumes ONTAP can access the software image.

   > The predefined Cloud Volumes ONTAP security group allows outbound HTTP connections by default.

3. Obtain the software image from the NetApp Support Site.

4. Copy the software image to a directory on the Connector or on an HTTP server from which the file will be served.

   Two paths are available. The correct path depends on your Connector version.

   ° `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`

   ° `/opt/application/netapp/cloudmanager/ontap/images/`

5. From the working environment in Cloud Manager, click the menu icon, and then click **Advanced > Update Cloud Volumes ONTAP**.

6. On the update software page, enter the URL, and then click **Change Image**.

   If you copied the software image to the Connector in the path shown above, you would enter the following URL:

   http://<Connector-private-IP-address>/ontap/images/<image-file-name>

7. Click **Proceed** to confirm.

Result

Cloud Manager starts the software update. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

Registering pay-as-you-go systems

Support from NetApp is included with Cloud Volumes ONTAP PAYGO systems, but you must first activate support by registering the systems with NetApp.

Registering a PAYGO system with NetApp is required to upgrade ONTAP software using any of the methods described on this page.

A system that isn't registered for support will still receive the software update notifications that appear in Cloud Manager when a new version is available. But you will need to register the system before you can upgrade the software.

Steps

1. If you have not yet added your NetApp Support Site account to Cloud Manager, go to **Account Settings** and add it now.

   Learn how to add NetApp Support Site accounts.

2. On the Canvas page, double-click the name of the system that you want to register.

3. Click the menu icon and then click **Support registration**:

4. Select a NetApp Support Site account and click **Register**.

Result

Cloud Manager registers the system with NetApp.

Managing the state of Cloud Volumes ONTAP

You can stop and start Cloud Volumes ONTAP from Cloud Manager to manage your cloud compute costs.

Scheduling automatic shutdowns of Cloud Volumes ONTAP

You might want to shut down Cloud Volumes ONTAP during specific time intervals to lower your compute costs. Rather than do this manually, you can configure Cloud Manager to automatically shut down and then restart systems at specific times.

About this task

- When you schedule an automatic shutdown of your Cloud Volumes ONTAP system, Cloud Manager postpones the shutdown if an active data transfer is in progress.

  Cloud Manager shuts down the system after the transfer is complete.

- This task schedules automatic shutdowns of both nodes in an HA pair.

- Snapshots of boot and root disks are not created when turning off Cloud Volumes ONTAP through scheduled shutdowns.

Snapshots are automatically created only when performing a manual shutdown, as described in the next section.

Steps

1. From the working environment, click the clock icon:

🕘

2. Specify the shutdown schedule:

   a. Choose whether you want to shut down the system every day, every weekday, every weekend, or any combination of the three options.

   b. Specify when you want to turn off the system and for how long you want it turned off.

   Example

   The following image shows a schedule that instructs Cloud Manager to shut down the system every Saturday at 12:00 a.m. for 48 hours. Cloud Manager restarts the system every Monday at 12:00 a.m.

| ☐ **Turn off every weekday**
Mon, Tue, Wed, Thu, Fri | turn off at | 08 : 00 PM | for 12 | Hours (1-24) |
| ☑ **Turn off every weekend**
Sat | turn off at | 12 : 00 AM | for 48 | Hours (1-48) |

3. Click **Save**.

Result

Cloud Manager saves the schedule. The clock icon changes to indicate that a schedule is set: ✅🕘

Stopping Cloud Volumes ONTAP

Stopping Cloud Volumes ONTAP saves you from accruing compute costs and creates snapshots of the root and boot disks, which can be helpful for troubleshooting.

> ℹ️ To reduce costs, Cloud Manager periodically deletes older snapshots of root and boot disks. Only the two most recent snapshots are retained for both the root and boot disks.

About this task

When you stop an HA pair, Cloud Manager shuts down both nodes.

Steps

1. From the working environment, click the **Turn off** icon.

🛡️ ☸️ [⏻] ↻ 🕘 〰️ ☰

2. Keep the option to create snapshots enabled because the snapshots can enable system recovery.

3. Click **Turn Off**.

   It can take up to a few minutes to stop the system. You can restart systems at a later time from the working environment page.

Synchronize the system time using NTP

Specifying an NTP server synchronizes the time between the systems in your network, which can help prevent issues due to time differences.

Specify an NTP server using the Cloud Manager API or from the user interface when you create a CIFS server.

Modify system write speed

Cloud Manager enables you to choose a normal or high write speed for Cloud Volumes ONTAP. The default write speed is normal. You can change to high write speed if fast write performance is required for your workload.

High write speed is supported with all types of single node systems and some HA pair configurations. View supported configurations in the Cloud Volumes ONTAP Release Notes

Before you change the write speed, you should understand the differences between the normal and high settings.

About this task

- Ensure that operations such as volume or aggregate creation are not in progress.

- Be aware that this change restarts the Cloud Volumes ONTAP system. This is disruptive process that requires downtime for the entire system.

Steps

1. From the working environment, click the menu icon, and then click **Advanced > Writing Speed**.

2. Select **Normal** or **High**.

   If you choose High, then you'll need to read the "I understand…" statement and confirm by checking the box.

3. Click **Save**, review the confirmation message, and then click **Proceed**.

Change the password for Cloud Volumes ONTAP

Cloud Volumes ONTAP includes a cluster admin account. You can change the password for this account from Cloud Manager, if needed.

> ⚠ You should not change the password for the admin account through System Manager or the CLI. The password will not be reflected in Cloud Manager. As a result, Cloud Manager cannot monitor the instance properly.

Steps

1. From the working environment, click the menu icon, and then click **Advanced > Set password**.
2. Enter the new password twice and then click **Save**.

   The new password must be different than one of the last six passwords that you used.

Add, remove, or delete systems

Adding existing Cloud Volumes ONTAP systems to Cloud Manager

You can discover and add existing Cloud Volumes ONTAP systems to Cloud Manager. You might do this if you deployed a new Cloud Manager system.

Before you begin

You must know the password for the Cloud Volumes ONTAP admin user account.

Steps

1. On the Canvas page, click **Add Working Environment**.
2. Select the cloud provider in which the system resides.
3. Choose the type of Cloud Volumes ONTAP system.
4. Click the link to discover an existing system.
5. On the Region page, choose the region where the instances are running, and then select the instances.
6. On the Credentials page, enter the password for the Cloud Volumes ONTAP admin user, and then click **Go**.

Result

Cloud Manager adds the Cloud Volumes ONTAP instances to the workspace.

Removing Cloud Volumes ONTAP working environments

The Account Admin can remove a Cloud Volumes ONTAP working environment to move it to another system or to troubleshoot discovery issues.

About this task

Removing a Cloud Volumes ONTAP working environment removes it from Cloud Manager. It does not delete the Cloud Volumes ONTAP system. You can later rediscover the working environment.

Removing a working environment from Cloud Manager enables you to do the following:

- Rediscover it in another workspace
- Rediscover it from another Cloud Manager system
- Rediscover it if you had problems during the initial discovery

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Tools**.

2. From the Tools page, click **Launch**.

3. Select the Cloud Volumes ONTAP working environment that you want to remove.

4. On the Review and Approve page, click **Go**.

Result

Cloud Manager removes the working environment. Users can rediscover this working environment from the Canvas page at any time.

Deleting a Cloud Volumes ONTAP system

You should always delete Cloud Volumes ONTAP systems from Cloud Manager, rather than from your cloud provider's console. For example, if you terminate a licensed Cloud Volumes ONTAP instance from your cloud provider, then you can't use the license key for another instance. You must delete the working environment from Cloud Manager to release the license.

When you delete a working environment, Cloud Manager terminates Cloud Volumes ONTAP instances and deletes disks and snapshots.

Resources managed by other services like backups for Cloud Backup and instances for Cloud Data Sense and Monitoring are not deleted when you delete a working environment. You'll need to manually delete them yourself. If you don't, then you'll continue to receive charges for these resources.

> ⓘ When Cloud Manager deploys Cloud Volumes ONTAP in your cloud provider, it enables termination protection on the instances. This option helps prevent accidental termination.

Steps

1. If you enabled Cloud Backup on the working environment, determine whether the backed up data is still required and then delete the backups, if necessary.

   Cloud Backup is independent from Cloud Volumes ONTAP by design. Cloud Backup doesn't automatically delete backups when you delete a Cloud Volumes ONTAP system, and there is no current support in the UI to delete the backups after the system has been deleted.

2. If you enabled Cloud Data Sense or Monitoring on this working environment and no other working environments use those services, then you'll need to delete the instances for those services.

   ◦ Learn more about the Cloud Data Sense instance.

   ◦ Learn more about the Monitoring Acquisition Unit.

3. Delete the Cloud Volumes ONTAP working environment.

   a. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment that you want to delete.

   b. Click menu icon and then click **Delete**.

c. Type the name of the working environment and then click **Delete**.

It can take up to 5 minutes to delete the working environment.

Azure administration

Change the Azure VM type for Cloud Volumes ONTAP

You can choose from several VM types when you launch Cloud Volumes ONTAP in Microsoft Azure. You can change the VM type at any time if you determine that it is undersized or oversized for your needs.

About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

  ONTAP 9 Documentation: Commands for configuring automatic giveback

- Changing the VM type can affect Microsoft Azure service charges.

- The operation restarts Cloud Volumes ONTAP.

 For single node systems, I/O is interrupted.

  For HA pairs, the change is nondisruptive. HA pairs continue to serve data.

  > Cloud Manager gracefully changes one node at a time by initiating takeover and waiting for give back. NetApp's QA team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, we did see retries on the I/O level, but the application layer overcame these short "re-wire" of NFS/CIFS connections.

Steps

1. From the Canvas, select the working environment.

2. In the right pane, click the menu icon and select **Optimize Cost & Performance**.
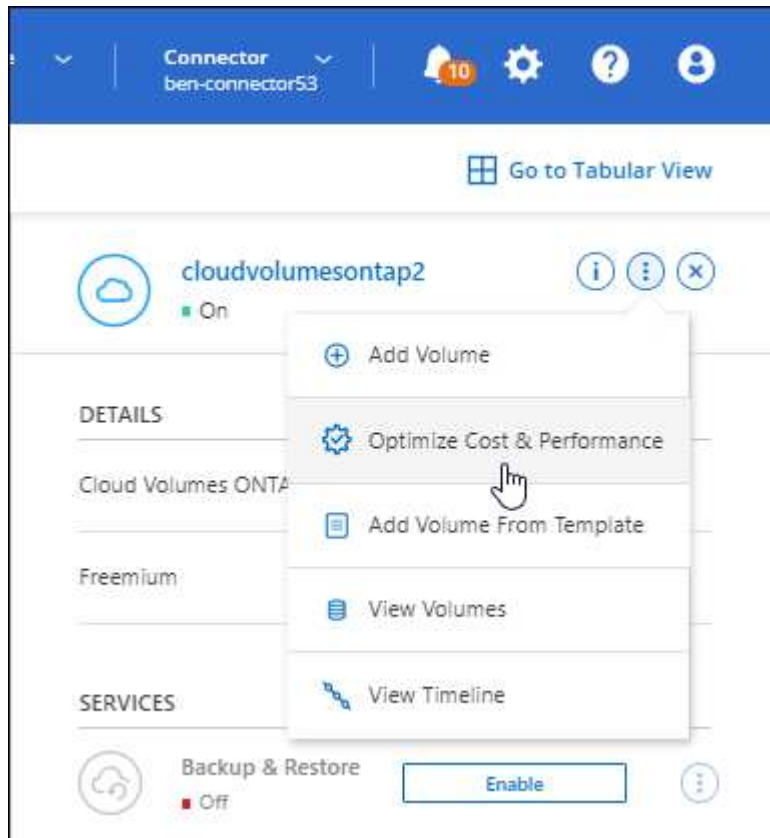
> 💡 This option is also available by entering the working environment, opening the action menu, and selecting **Change VM**.

3. If you are using a node-based PAYGO license, you can optionally choose a different license.

4. Select a VM type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

Result

Cloud Volumes ONTAP reboots with the new configuration.

Overriding CIFS locks for Cloud Volumes ONTAP HA pairs in Azure

The Account Admin can enable a setting in Cloud Manager that prevents issues with Cloud Volumes ONTAP storage giveback during Azure maintenance events. When you enable this setting, Cloud Volumes ONTAP vetoes CIFS locks and resets active CIFS sessions.

About this task

Microsoft Azure schedules periodic maintenance events on its virtual machines. When a maintenance event occurs on a Cloud Volumes ONTAP HA pair, the HA pair initiates storage takeover. If there are active CIFS sessions during this maintenance event, the locks on CIFS files can prevent storage giveback.

If you enable this setting, Cloud Volumes ONTAP will veto the locks and reset the active CIFS sessions. As a result, the HA pair can complete storage giveback during these maintenance events.

> ⚠️ This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

What you'll need

You need to create a Connector before you can change Cloud Manager settings. Learn how.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.

2. Under **Azure**, click **Azure CIFS locks for Azure HA working environments**.

3. Click the checkbox to enable the feature and then click **Save**.

Use an Azure Private Link or service endpoints

Cloud Volumes ONTAP uses an Azure Private Link for connections to its associated storage accounts. If needed, you can disable Azure Private Links and use service endpoints instead.

Overview

By default, Cloud Manager enables an Azure Private Link for connections between Cloud Volumes ONTAP and its associated storage accounts. An Azure Private Link secures connections between endpoints in Azure and provides performance benefits.

If required, you can configure Cloud Volumes ONTAP to use service endpoints instead of an Azure Private Link.

With either configuration, Cloud Manager always limits network access for connections between Cloud Volumes ONTAP and storage accounts. Network access is limited to the VNet where Cloud Volumes ONTAP is deployed and the VNet where the Connector is deployed.

Disable Azure Private Links and use service endpoints instead

If required by your business, you can change a setting in Cloud Manager so that it configures Cloud Volumes ONTAP to use service endpoints instead of an Azure Private Link. Changing this setting applies to new Cloud Volumes ONTAP systems that you create.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Connector Settings**.

2. Under **Azure**, click **Use Azure Private Link**.

3. Deselect **Private Link connection between Cloud Volumes ONTAP and storage accounts**.

4. Click **Save**.

Work with Azure Private Links

In most cases, there's nothing that you need to do to set up Azure Private links with Cloud Volumes ONTAP. Cloud Manager manages Azure Private Links for you. But if you use Azure Private DNS, then you'll need to edit a configuration file. You should also be aware of a requirement for the Connector location in Azure.

How Private Link connections work

When Cloud Manager deploys Cloud Volumes ONTAP in Azure, it creates a private endpoint in the resource group. The private endpoint is associated with storage accounts for Cloud Volumes ONTAP. As a result, access to Cloud Volumes ONTAP storage travels through the Microsoft backbone network.

Client access goes through the private link when clients are within the same VNet as Cloud Volumes ONTAP, within peered VNets, or in your on-premises network when using a private VPN or ExpressRoute connection to the VNet.

Here's an example that shows client access over a private link from within the same VNet and from an on-prem network that has either a private VPN or ExpressRoute connection.
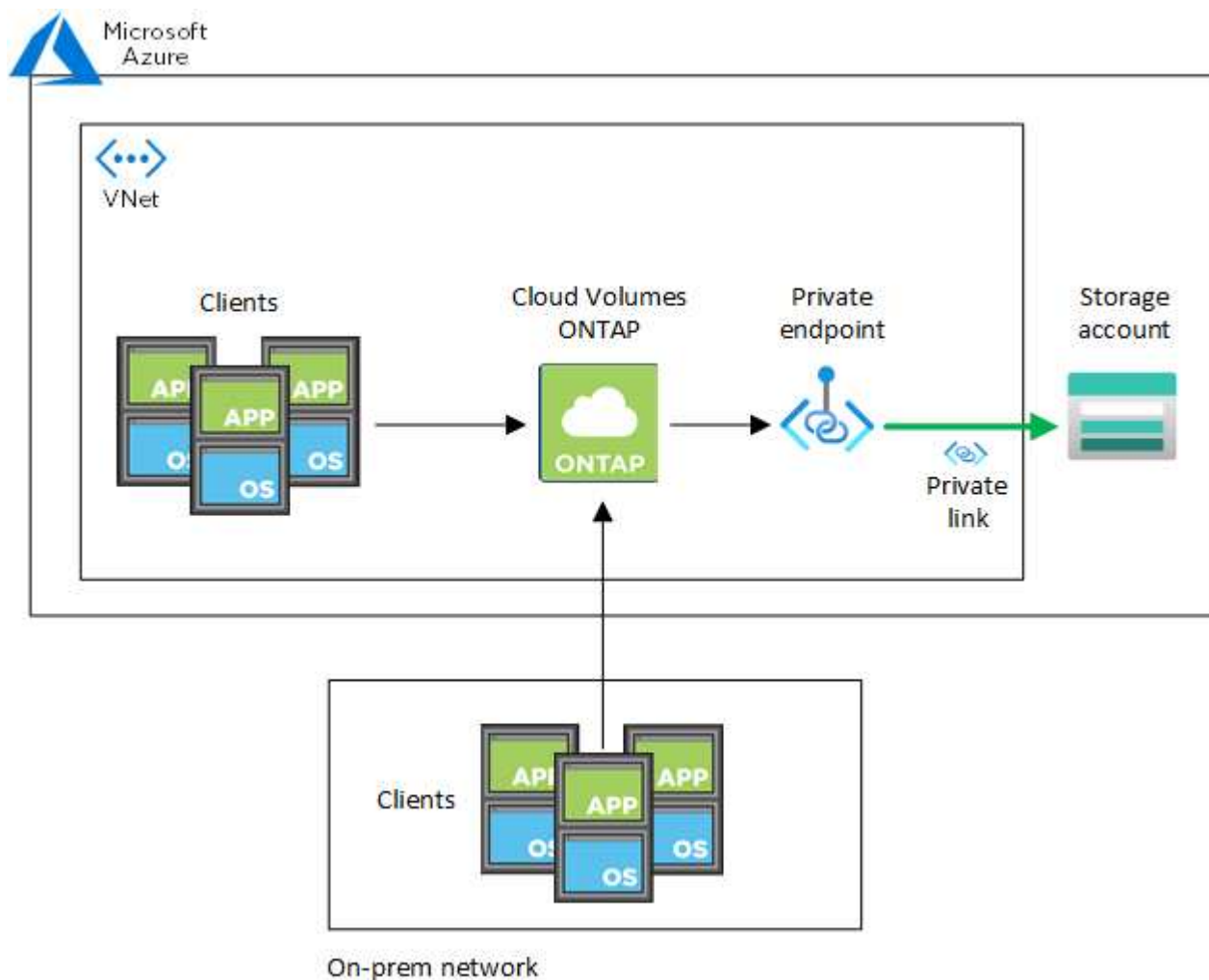
Connector location in Azure

The Connector should be deployed in the same Azure region as the Cloud Volumes ONTAP systems that it manages, or in the Azure region pair for the Cloud Volumes ONTAP systems. This requirement ensures that an Azure Private Link connection is used between Cloud Volumes ONTAP and its associated storage accounts.

Provide Cloud Manager with details about your Azure Private DNS

If you use Azure Private DNS, then you need to modify a configuration file on each Connector. Otherwise, Cloud Manager can't enable the Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts.

Note that the DNS name must match Azure DNS naming requirements as shown in Azure documentation.

Steps

1. SSH to the Connector host and log in.

2. Navigate to the following directory: /opt/application/netapp/cloudmanager/docker_occm/data

3. Edit app.conf by adding the "user-private-dns-zone-settings" parameter with the following keyword-value pairs:

```
"user-private-dns-zone-settings" : {
    "resource-group" : "<resource group name of the DNS zone>",
    "subscription" : "<subscription ID>",
    "use-existing" : true
}
```

The parameter should be entered at the same level as "system-id" like shown below:

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

Note that the subscription keyword is required only if the Private DNS Zone exists in a different subscription than the Connector.

4. Save the file and log off the Connector.

   A reboot isn't required.

Enable rollback on failures

If Cloud Manager fails to create an Azure Private Link as part of specific actions, it completes the action without the Azure Private Link connection. This can happen when creating a new working environment (single node or HA pair), or when the following actions occur on an HA pair: creating a new aggregate, adding disks to an existing aggregate, or creating a new storage account when going above 32 TiB.

You can change this default behavior by enabling rollback if Cloud Manager fails to create the Azure Private Link. This can help to ensure that you're fully compliant with your company's security regulations.

If you enable rollback, Cloud Manager stops the action and rolls back all resources that were created as part of the action.

Enabling rollback is supported through the API only.

Step

1. Use the `PUT /occm/config` API call with the following request body:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

Administer Cloud Volumes ONTAP using the Advanced View

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using ONTAP System Manager, which is a management interface that's provided with an ONTAP system. We have included the System Manager interface directly inside Cloud Manager so that you don't need to leave Cloud Manager for advanced management.

This Advanced View is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Features

The Advanced View in Cloud Manager gives you access to additional management features:

- Advanced storage management

  Manage consistency groups, shares, qtrees, quotas, and Storage VMs.

- Networking management

  Manage IPspaces, network interfaces, portsets, and ethernet ports.

- Events and jobs

  View event logs, system alerts, jobs, and audit logs.

- Advanced data protection

  Protect storage VMs, LUNs, and consistency groups.

- Host management

  Set up SAN initiator groups and NFS clients.

Supported configurations

Advanced management through System Manager is supported with Cloud Volumes ONTAP 9.10.0 and later in standard cloud regions.

System Manager integration is not supported in GovCloud regions or in regions that have no outbound internet access.

Limitations

A few features that appear in the System Manager interface are not supported with Cloud Volumes ONTAP:

- Cloud Tiering

  The Cloud Tiering service is not supported with Cloud Volumes ONTAP. Tiering data to object storage must

be set up directly from Cloud Manager's Standard View when creating volumes.

- Tiers

  Aggregate management (including local tiers and cloud tiers) is not supported from System Manager. You must manage aggregates directly from Cloud Manager's Standard View.

- Firmware upgrades

  Automatic firmware updates from the **Cluster > Settings** page is not supported with Cloud Volumes ONTAP.
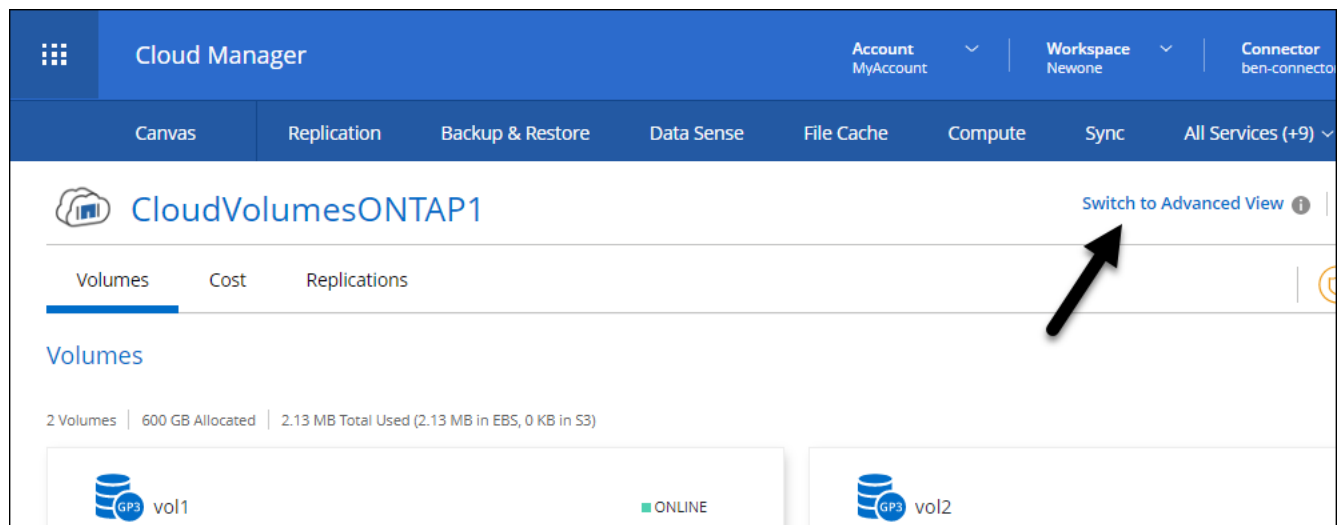
In addition, role-based access control from System Manager is not supported.

How to get started

Open a Cloud Volumes ONTAP working environment and click the Advanced View option.

Steps

1. On the Canvas page, double-click the name of a Cloud Volumes ONTAP system.
2. In the top-right, click **Switch to Advanced View**.

3. If the confirmation message appears, read through it and click **Close**.
4. Use System Manager to manage Cloud Volumes ONTAP.
5. If needed, click **Switch to Standard View** to return to standard management through Cloud Manager.

Help with using System Manager

If you need help using System Manager with Cloud Volumes ONTAP, you can refer to ONTAP documentation for step-by-step instructions. Here are a few links that might help:

- Volume and LUN management
- Network management
- Data protection

Administer Cloud Volumes ONTAP from the CLI

The Cloud Volumes ONTAP CLI enables you to run all administrative commands and is a good choice for advanced tasks or if you are more comfortable using the CLI. You can connect to the CLI using Secure Shell (SSH).

Before you begin

The host from which you use SSH to connect to Cloud Volumes ONTAP must have a network connection to Cloud Volumes ONTAP. For example, you might need to SSH from a jump host that's in your cloud provider network.

Steps

1. In Cloud Manager, identify the IP address of the cluster management interface:
   a. On the Canvas page, select the Cloud Volumes ONTAP system.
   b. Copy the cluster management IP address that appears in the right pane.

2. Use SSH to connect to the cluster management interface IP address using the admin account.

   Example

   The following image shows an example using PuTTY:

3. At the login prompt, enter the password for the admin account.

Example

```
Password: ********
COT2::>
```

System health and events

Verify AutoSupport setup

AutoSupport proactively monitors the health of your system and sends messages to NetApp technical support. By default, AutoSupport is enabled on each node to send messages to technical support using the HTTPS transport protocol. It's best to verify that AutoSupport can send these messages.

The only required configuration step is to ensure that Cloud Volumes ONTAP has outbound internet connectivity. For details, refer to the networking requirements for your cloud provider.

AutoSupport requirements

Cloud Volumes ONTAP nodes require outbound internet access for NetApp AutoSupport, which proactively monitors the health of your system and sends messages to NetApp technical support.

Routing and firewall policies must allow HTTP/HTTPS traffic to the following endpoints so Cloud Volumes ONTAP can send AutoSupport messages:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

If an outbound internet connection isn't available to send AutoSupport messages, Cloud Manager automatically configures your Cloud Volumes ONTAP systems to use the Connector as a proxy server. The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you defined strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

After you've verified that outbound internet access is available, you can test AutoSupport to ensure that it can send messages. For instructions, refer to ONTAP docs: Set up AutoSupport.

Troubleshoot your AutoSupport configuration

If an outbound connection isn't available and Cloud Manager can't configure your Cloud Volumes ONTAP system to use the Connector as a proxy server, you'll receive a notification from Cloud Manager titled "<working environment name> is unable to send AutoSupport messages."

You're most likely receiving this message because of networking issues.

Follow these steps to address this problem.

Steps

1. SSH to the Cloud Volumes ONTAP system so that you can administer the system from the CLI.

   Learn how to SSH to Cloud Volumes ONTAP.

2. Display the detailed status of the AutoSupport subsystem:

   `autosupport check show-details`

   The response should be similar to the following:

```
    Category: smtp
          Component: mail-server
             Status: failed
             Detail: SMTP connectivity check failed for destination:
                     mailhost. Error: Could not resolve host -
 'mailhost'
            Corrective Action: Check the hostname of the SMTP server


    Category: http-https
        Component: http-put-destination
            Status: ok
            Detail: Successfully connected to:
                    <https://support.netapp.com/put/AsupPut/>.


        Component: http-post-destination
            Status: ok
            Detail: Successfully connected to:

 https://support.netapp.com/asupprod/post/1.0/postAsup.


    Category: on-demand
          Component: ondemand-server
             Status: ok
             Detail: Successfully connected to:
                     https://support.netapp.com/aods/asupmessage.


    Category: configuration
           Component: configuration
               Status: ok
               Detail: No configuration issues found.
    5 entries were displayed.
```

If the status of the http-https category is "ok" then it means AutoSupport is configured properly and messages can be sent.

3. If the status is not ok, verify the proxy URL for each Cloud Volumes ONTAP node:

```
autosupport show -fields proxy-url
```

4. If the proxy URL parameter is empty, configure Cloud Volumes ONTAP to use the Connector as a proxy:

```
autosupport modify -proxy-url http://<connector private ip>:3128
```

5. Verify AutoSupport status again:

```
autosupport check show-details
```

6. If the status is still is failed, validate that there is connectivity between Cloud Volumes ONTAP and the Connector over port 3128.

7. If the status ID is still failed after verifying that there is connectivity, SSH to the Connector.

   [Learn more about Connecting to the Linux VM for the Connector](#)

8. Go to `/opt/application/netapp/cloudmanager/docker_occm/data/`

9. Open the proxy configuration file `squid.conf`

   The basic structure of the file is as follows:

   ```
   http_port 3128
   acl localnet src 172.31.0.0/16
   acl azure_aws_metadata dst 169.254.169.254

   http_access allow localnet
   http_access deny azure_aws_metadata
   http_access allow localhost
   http_access deny all
   ```

   The localnet src value is the CIDR of the Cloud Volumes ONTAP system.

10. If the CIDR block of the Cloud Volumes ONTAP system isn't in the range that's specified in the file, either update the value or add a new entry as follows:

    `acl cvonet src <cidr>`

    If you add this new entry, don't forget to also add an allow entry:

    `http_access allow cvonet`

    Here's an example:

    ```
    http_port 3128
    acl localnet src 172.31.0.0/16
    acl cvonet src 172.33.0.0/16
    acl azure_aws_metadata dst 169.254.169.254

    http_access allow localnet
    http_access allow cvonet
    http_access deny azure_aws_metadata
    http_access allow localhost
    http_access deny all
    ```

11. After editing the config file, restart the proxy container as sudo:

    `docker restart squid`

12. Go back to the Cloud Volumes ONTAP CLI and verify that Cloud Volumes ONTAP can send AutoSupport messages:

```
autosupport check show-details
```

Configure EMS

The Event Management System (EMS) collects and displays information about events that occur on ONTAP systems. To receive event notifications, you can set event destinations (email addresses, SNMP trap hosts, or syslog servers) and event routes for a particular event severity.

You can configure EMS using the CLI. For instructions, refer to ONTAP docs: EMS configuration overview.

Concepts

Cloud Volumes ONTAP licensing

Several licensing options are available for Cloud Volumes ONTAP. Each option enables you to choose a consumption model that meets your needs.

Licensing overview

The following licensing options are available for new customers.

Capacity-based licensing

Pay for multiple Cloud Volumes ONTAP systems in your NetApp account by provisioned capacity. Includes the ability to purchase add-on cloud data services.

Keystone Flex Subscription

A pay-as-you-grow subscription-based service that delivers a seamless hybrid cloud experience for HA pairs.

The previous by-node licensing model remains available for existing customers who have already purchased a license or who have an active marketplace subscription.

The following sections provide more details about each of these options.

Capacity-based licensing

Capacity-based licensing packages enable you to pay for Cloud Volumes ONTAP per TiB of capacity. The license is associated with your NetApp account and enables you to charge multiple systems against the license, as long as enough capacity is available through the license.

For example, you could purchase a single 20 TiB license, deploy four Cloud Volumes ONTAP systems, and then allocate a 5 TiB volume to each system, for a total of 20 TiB. The capacity is available to the volumes on each Cloud Volumes ONTAP system deployed in that account.

Capacity-based licensing is available in the form of a *package*. When you deploy a Cloud Volumes ONTAP system, you can choose from several licensing packages based on your business needs.

Packages

The following capacity-based packages are available for Cloud Volumes ONTAP.

Freemium

Provides all Cloud Volumes ONTAP features free of charge from NetApp (cloud provider charges still apply).

- No license or contract is needed.
- Support from NetApp is not included.
- You're limited to 500 GiB of provisioned capacity per Cloud Volumes ONTAP system.
- You can use up to 10 Cloud Volumes ONTAP systems with the Freemium offering per NetApp account, in any cloud provider.

- If the provisioned capacity for a Cloud Volumes ONTAP system exceeds 500 GiB, Cloud Manager converts the system to the Essentials package.

  As soon as a system is converted to the Essentials package, the minimum charge applies.

  Any other systems that have less than 500 GiB of provisioned capacity stay on Freemium (as long as they were deployed using the Freemium offering).

Optimized

Pay for provisioned capacity and I/O operations separately.

- Cloud Volumes ONTAP single node or HA
- Charging is based on two cost components: storage and usage (I/O)

  You will not be charged for I/O related to data replication (SnapMirror) or NDMP.

- Available only in the Azure Marketplace as a pay-as-you-go offering or as an annual contract
- Supported with selected VM types: E4s_v3, E4ds_v4, DS4_v2, DS13_v2, E8s_v3, and E8ds_v4
- Add on any of NetApp's cloud data services at extra cost

Essentials

Pay by capacity for Cloud Volumes ONTAP in a number of different configurations.

- Choose your Cloud Volumes ONTAP configuration:
  - A single node or HA system
  - File and block storage or secondary data for disaster recovery (DR)
- Add on any of NetApp's cloud data services at extra cost

Professional

Pay by capacity for any type of Cloud Volumes ONTAP configuration with unlimited backups.

- Provides licensing for any Cloud Volumes ONTAP configuration

  Single node or HA with capacity charging for primary and secondary volumes at the same rate

- Includes unlimited volume backups using Cloud Backup, but only for Cloud Volumes ONTAP systems deployed with the Professional package
- Add on any of NetApp's cloud data services at extra cost

Edge Cache

Provides licensing for Cloud Volumes Edge Cache.

- The same capabilities as the Professional package with business continuity and data protection for a distributed enterprise
- Intelligent edge caching through a small-footprint Windows VM at each location
- 30 TiB minimum with six edge nodes included

- One edge node with every 3 TiBs of additional capacity purchased
- Available only in the Azure Marketplace as a pay-as-you-go offering or as an annual contract

Learn more about how Cloud Volumes Edge Cache can help your business

Consumption models

Capacity-based licensing packages are available with the following consumption models:

- **BYOL**: A license purchased from NetApp that can be used to deploy Cloud Volumes ONTAP in any cloud provider.

  Note that the Optimized and Edge Cache packages are not available with BYOL.

- **PAYGO**: An hourly subscription from your cloud provider's marketplace.
- **Annual**: An annual contract from your cloud provider's marketplace.

Note the following:

- If you purchase a license from NetApp (BYOL), you also need to subscribe to the PAYGO offering from your cloud provider's marketplace.

  Your license is always charged first, but you'll be charged from the hourly rate in the marketplace in these cases:

  - If you exceed your licensed capacity
  - If the term of your license expires
- If you have an annual contract from a marketplace, *all* Cloud Volumes ONTAP systems that you deploy are charged against that contract. You can't mix and match an annual marketplace contract with BYOL.

Changing packages

After deployment, you can change the package for a Cloud Volumes ONTAP system that uses capacity-based licensing. For example, if you deployed a Cloud Volumes ONTAP system with the Essentials package, you can change it to the Professional package if your business needs changed.

Learn how to change charging methods.

Pricing

For details about pricing, go to NetApp Cloud Central.

Free trials

A 30-day free trial is available from the pay-as-you-go subscription in your cloud provider's marketplace. The free trial includes Cloud Volumes ONTAP and Cloud Backup. The trial starts when you subscribe to the offering in the marketplace.

There are no instance or capacity limitations. You can deploy as many Cloud Volumes ONTAP systems as you'd like and allocate as much capacity as needed, free of charge for 30 days. The free trial automatically converts to a paid hourly subscription after 30 days.

There are no hourly software license charges for Cloud Volumes ONTAP, but infrastructure charges from your

cloud provider still apply.

> 💡 You will receive a notification in Cloud Manager when the free trial starts, when there are 7 days left, and when there is 1 day remaining. For example:
>
> ⓘ **Your Cloud Manager free trial is almost over (7 days left)**
>
> 23 minutes ago | Digital Wallet

Supported configurations

Capacity-based licensing packages are available with Cloud Volumes ONTAP 9.7 and later.

Capacity limit

With this licensing model, each individual Cloud Volumes ONTAP system supports up to 2 PiB of capacity through disks and tiering to object storage.

There is no maximum capacity limitation when it comes to the license itself.

Max number of systems

With capacity-based licensing, the maximum number of Cloud Volumes ONTAP systems is limited to 20 per NetApp account. A *system* is a Cloud Volumes ONTAP HA pair, a Cloud Volumes ONTAP single node system, or any additional storage VMs that you create. The default storage VM does not count against the limit. This limit applies to all licensing models.

For example, let's say you have three working environments:

- A single node Cloud Volumes ONTAP system with one storage VM (this is the default storage VM that's created when you deploy Cloud Volumes ONTAP)

  This working environment counts as one system.

- A single node Cloud Volumes ONTAP system with two storage VMs (the default storage VM, plus one additional storage VM that you created)

  This working environment counts as two systems: one for the single node system and one for the additional storage VM.

- A Cloud Volumes ONTAP HA pair with three storage VMs (the default storage VM, plus two additional storage VMs that you created)

  This working environment counts as three systems: one for the HA pair and two for the additional storage VMs.

That's six systems in total. You would then have room for an additional 14 systems in your account.

If you have a large deployment that requires more then 20 systems, contact your account rep or sales team.

Learn more about NetApp accounts.

Notes about charging

The following details can help you understand how charging works with capacity-based licensing.

Minimum charge

There is a 4 TiB minimum charge for each data-serving storage VM that has least one primary (read-write) volume. If the sum of the primary volumes is less than 4 TiB, then Cloud Manager applies the 4 TiB minimum charge to that storage VM.

If you haven't provisioned any volumes yet, then the minimum charge doesn't apply.

The 4 TiB minimum capacity charge doesn't apply to storage VMs that contain secondary (data protection) volumes only. For example, if you have a storage VM with 1 TiB of secondary data, then you're charged just for that 1 TiB of data.

Overages

If you exceed your BYOL capacity or if your license expires, you'll be charged for overages at the hourly rate based on your marketplace subscription.

Essentials package

With the Essentials package, you're billed by the deployment type (HA or single node) and the volume type (primary or secondary). For example, *Essentials HA* has different pricing than *Essentials Secondary HA*.

If you purchased an Essentials license from NetApp (BYOL) and you exceed the licensed capacity for that deployment and volume type, the Digital Wallet charges overages against a higher priced Essentials license (if you have one). This happens because we first use the available capacity that you've already purchased as prepaid capacity before charging against the marketplace. Charging to the marketplace would add costs to your monthly bill.

Here's an example. Let's say you have the following licenses for the Essentials package:

- A 500 TiB *Essentials Secondary HA* license that has 500 TiB of committed capacity
- A 500 TiB *Essentials Single Node* license that only has 100 TiB of committed capacity

Another 50 TiB is provisioned on an HA pair with secondary volumes. Instead of charging that 50 TiB to PAYGO, the Digital Wallet charges the 50 TiB overage against the *Essentials Single Node* license. That license is priced higher than *Essentials Secondary HA*, but it's cheaper than the PAYGO rate.

In the Digital Wallet, that 50 TiB will be shown as charged against the *Essentials Single Node* license.

Storage VMs

- There are no extra licensing costs for additional data-serving storage VMs (SVMs), but there is a 4 TiB minimum capacity charge per data-serving SVM.
- Disaster recovery SVMs are charged according to the provisioned capacity.

HA pairs

For HA pairs, you're only charged for the provisioned capacity on a node. You aren't charged for data that is synchronously mirrored to the partner node.

FlexClone and FlexCache volumes

- You won't be charged for the capacity used by FlexClone volumes.

- Source and destination FlexCache volumes are considered primary data and charged according to the provisioned space.

How to get started

Learn how to get started with capacity-based licensing:

- Set up licensing for Cloud Volumes ONTAP in Azure

Keystone Flex Subscription

A pay-as-you-grow subscription-based service that delivers a seamless hybrid cloud experience for those preferring OpEx consumption models to upfront CapEx or leasing.

Charging is based on the size of your committed capacity for one or more Cloud Volumes ONTAP HA pairs in your Keystone Flex Subscription.

The provisioned capacity for each volume is aggregated and compared to the committed capacity on your Keystone Flex Subscription periodically, and any overages are charged as burst on your Keystone Flex Subscription.

Learn more about Keystone Flex Subscriptions.

Supported configurations

Keystone Flex Subscriptions are supported with HA pairs. This licensing option isn't supported with single node systems at this time.

Capacity limit

Each individual Cloud Volumes ONTAP system supports up to 2 PiB of capacity through disks and tiering to object storage.

How to get started

Learn how to get started with a Keystone Flex Subscription:

- Set up licensing for Cloud Volumes ONTAP in Azure

Node-based licensing

Node-based licensing is the previous generation licensing model that enabled you to license Cloud Volumes ONTAP by node. This licensing model is not available for new customers and no free trials are available. By-node charging has been replaced with the by-capacity charging methods described above.

Node-based licensing is still available for existing customers:

- If you have an active license, BYOL is available for license renewals only.

- If you have an active marketplace subscription, charging is still available through that subscription.

License conversions

Converting an existing Cloud Volumes ONTAP system to another licensing method isn't supported. The three current licensing methods are capacity-based licensing, Keystone Flex Subscriptions, and node-based licensing. For example, you can't convert a system from node-based licensing to capacity-based licensing (and vice versa).

If you want to transition to another licensing method, you can purchase a license, deploy a new Cloud Volumes ONTAP system using that license, and then replicate the data to that new system.

Note that converting a system from PAYGO by-node licensing to BYOL by-node licensing (and vice versa) isn't supported. You need to deploy a new system and then replicate data to that system. Learn how to change between PAYGO and BYOL.

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:

- Azure

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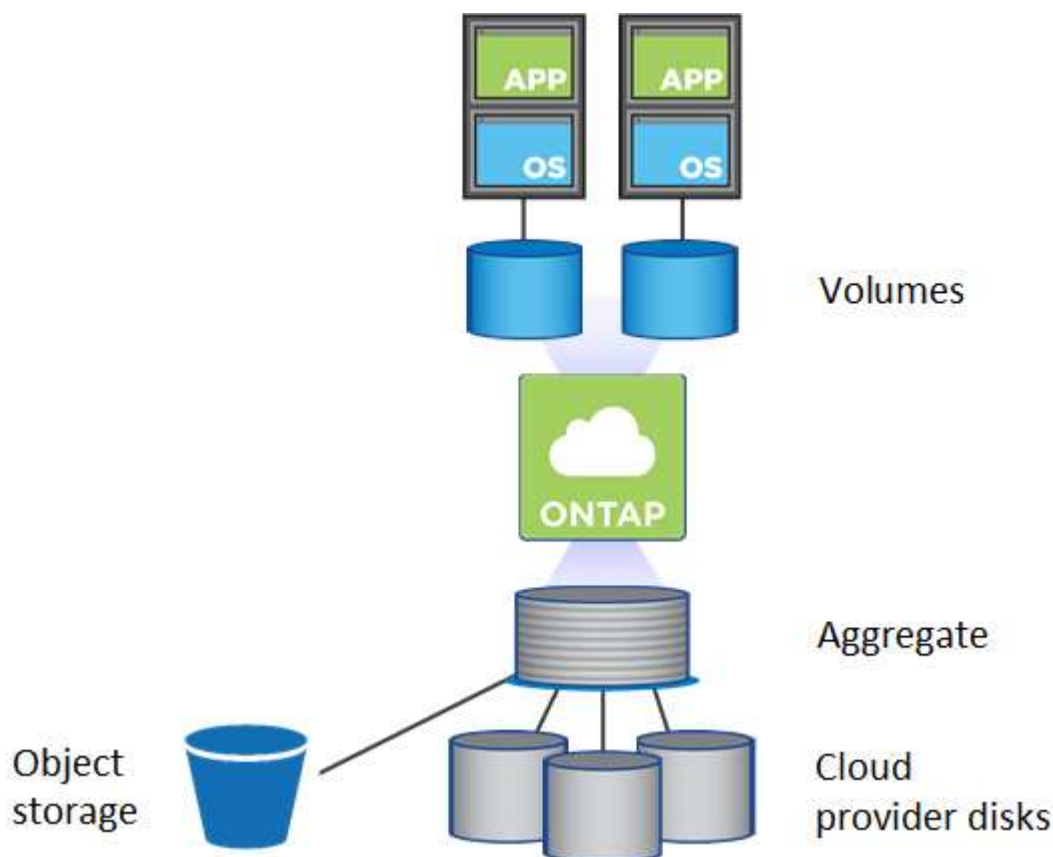
Several types of cloud disks are supported. You choose the disk type when you create a volume and the default disk size when you deploy Cloud Volumes ONTAP.

> 💡 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.

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 Premium page blobs, which have a maximum disk size of 8 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.

> ℹ️   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.

Cloud Manager 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.

Cloud Manager 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.

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.

- 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.

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.

- 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 provder 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.

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 9.11.0 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:

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.

High-availability pairs

High-availability pairs in Azure

A Cloud Volumes ONTAP high availability (HA) pair provides enterprise reliability and continuous operations in case of failures in your cloud environment. In Azure, storage is shared between the two nodes.

HA components

A Cloud Volumes ONTAP HA configuration in Azure includes the following components:

Note the following about the Azure components that Cloud Manager deploys for you:

Azure Standard Load Balancer

The load balancer manages incoming traffic to the Cloud Volumes ONTAP HA pair.

Availability Set

The Azure Availability Set is a logical grouping of the Cloud Volumes ONTAP nodes. The Availability Set ensures that the nodes are in different fault and update domains to provide redundancy and availability. Learn more about Availability Sets in the Azure docs.

Disks

Customer data resides on Premium Storage page blobs. Each node has access to the other node's storage. Additional storage is also required for boot, root, and core data.

Storage accounts

- One storage account is required for managed disks.

- One or more storage accounts are required for the Premium Storage page blobs, as the disk capacity limit per storage account is reached.

  Azure documentation: Azure Storage scalability and performance targets for storage accounts.

- One storage account is required for data tiering to Azure Blob storage.

- Starting with Cloud Volumes ONTAP 9.7, the storage accounts that Cloud Manager creates for HA pairs are general-purpose v2 storage accounts.

- You can enable an HTTPS connection from a Cloud Volumes ONTAP 9.7 HA pair to Azure storage accounts when creating a working environment. Note that enabling this option can impact write performance. You can't change the setting after you create the working environment.

RPO and RTO

An HA configuration maintains high availability of your data as follows:

- The recovery point objective (RPO) is 0 seconds.
  Your data is transactionally consistent with no data loss.

- The recovery time objective (RTO) is 60 seconds.
  In the event of an outage, data should be available in 60 seconds or less.

Storage takeover and giveback

Similar to a physical ONTAP cluster, storage in an Azure HA pair is shared between nodes. Connections to the partner's storage allows each node to access the other's storage in the event of a *takeover*. Network path failover mechanisms ensure that clients and hosts continue to communicate with the surviving node. The partner *gives back* storage when the node is brought back on line.

For NAS configurations, data IP addresses automatically migrate between HA nodes if failures occur.

For iSCSI, Cloud Volumes ONTAP uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.

ⓘ For information about which specific host configurations support ALUA, see the NetApp Interoperability Matrix Tool and the Host Utilities Installation and Setup Guide for your host operating system.

Storage takeover, resync, and giveback are all automatic by default. No user action is required.

Storage configurations

You can use an HA pair as an active-active configuration, in which both nodes serve data to clients, or as an active-passive configuration, in which the passive node responds to data requests only if it has taken over storage for the active node.

Actions unavailable during takeover

When a node in an HA pair isn't available, the other node serves data for its partner to provide continued data service. This is called *storage takeover*. Several actions are unavailable until in storage giveback is complete.

> 💡 When a node in an HA pair is unavailable, the state of the working environment in Cloud Manager is *Degraded*.

The following actions are unavailable from Cloud Manager during storage takeover:

- Support registration
- License changes
- Instance or VM type changes
- Write speed changes
- CIFS setup
- Changing the location of configuration backups
- Setting the cluster password
- Managing disks and aggregates (advanced allocation)

These actions are available again after storage giveback completes and the state of the working environment changes back to normal.

Security

Cloud Volumes ONTAP supports data encryption and provides protection against viruses and ransomware.

Encryption of data at rest

Cloud Volumes ONTAP supports the following encryption technologies:

- NetApp encryption solutions (NVE and NAE)
- Azure Storage Service Encryption

You can use NetApp encryption solutions with native encryption from your cloud provider, which encrypts data at the hypervisor level. Doing so would provide double encryption, which might be desired for very sensitive data. When the encrypted data is accessed, it's unencrypted twice—once at the hypervisor-level (using keys from the cloud provider) and then again using NetApp encryption solutions (using keys from an external key manager).

NetApp encryption solutions (NVE and NAE)

Cloud Volumes ONTAP supports NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE). NVE and NAE are software-based solutions that enable (FIPS) 140-2–compliant data-at-rest encryption of volumes. Both NVE and NAE use AES 256-bit encryption.

- NVE encrypts data at rest one volume a time. Each data volume has its own unique encryption key.

- NAE is an extension of NVE—it encrypts data for each volume, and the volumes share a key across the aggregate. NAE also allows common blocks across all volumes in the aggregate to be deduplicated.

Both NVE and NAE are supported with an external key manager.

If you use NVE, you have the option to use your cloud provider's key vault to protect ONTAP encryption keys:

- Azure Key Vault (AKV)

New aggregates have NetApp Aggregate Encryption (NAE) enabled by default after you set up an external key manager. New volumes that aren't part of an NAE aggregate will have NetApp Volume Encryption (NVE) enabled by default (for example, if you have existing aggregates that were created before setting up an external key manager).

Setting up a supported key manager is the only required step. For set up instructions, refer to Encrypting volumes with NetApp encryption solutions.

Azure Storage Service Encryption

Data is automatically encrypted on Cloud Volumes ONTAP in Azure using Azure Storage Service Encryption with a Microsoft-managed key.

You can use your own encryption keys if you prefer. Learn how to set up Cloud Volumes ONTAP to use a customer-managed key in Azure.

ONTAP virus scanning

You can use integrated antivirus functionality on ONTAP systems to protect data from being compromised by viruses or other malicious code.

ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

For information about the vendors, software, and versions supported by Vscan, see the NetApp Interoperability Matrix.

For information about how to configure and manage the antivirus functionality on ONTAP systems, see the ONTAP 9 Antivirus Configuration Guide.

Ransomware protection

Ransomware attacks can cost a business time, resources, and reputation. Cloud Manager enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

- Cloud Manager identifies volumes that are not protected by a Snapshot policy and enables you to activate the default Snapshot policy on those volumes.

  Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

- Cloud Manager also enables you to block common ransomware file extensions by enabling ONTAP's FPolicy solution.

[Learn how to implement the NetApp solution for ransomware](#).

Performance

You can review performance results to help you decide which workloads are appropriate for Cloud Volumes ONTAP.

Performance technical reports

- Cloud Volumes ONTAP for Microsoft Azure

  [NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads](#)

CPU performance

Cloud Volumes ONTAP nodes show as highly utilized (over 90%) from your cloud provider's monitoring tools. This is because ONTAP reserves all vCPUs presented to the virtual machine so that they are available when needed.

[Learn how to monitor Cloud Volumes ONTAP performance](#), or check out this [NetApp knowledgebase article about how to monitor ONTAP CPU utilization using the CLI](#)

License management for node-based BYOL

Each Cloud Volumes ONTAP system that has a node-based BYOL must have a system license installed with an active subscription. Cloud Manager simplifies the process by managing licenses for you and by displaying a warning before they expire.

> A node-based license is the previous generation BYOL for Cloud Volumes ONTAP. A node-based license is available for license renewals only.

[Learn more about Cloud Volumes ONTAP licensing options](#).

BYOL system licenses

A node-based license provides up to 368 TiB of capacity for a single node or HA pair.

You can purchase multiple licenses for a Cloud Volumes ONTAP BYOL system to allocate more than 368 TiB of capacity. For example, you might purchase two licenses to allocate up to 736 TiB of capacity to Cloud Volumes ONTAP. Or you could purchase four licenses to get up to 1.4 PiB.

The number of licenses that you can purchase for a single node system or HA pair is unlimited.

> ⓘ Some on-premises ONTAP storage systems that you purchased may have included a free Cloud Volumes ONTAP license. You can use the license to create a new Cloud Volumes ONTAP system, or you can apply the license to an existing Cloud Volumes ONTAP system to expand the capacity. See if you have any available licenses to use.

Be aware that disk limits can prevent you from reaching the capacity limit by using disks alone. You can go beyond the disk limit by tiering inactive data to object storage. For information about disk limits, refer to storage limits in the Cloud Volumes ONTAP Release Notes.

License management for a new system

When you create a node-based BYOL system, Cloud Manager prompts you for the serial number of your license and your NetApp Support Site account. Cloud Manager uses the account to download the license file from NetApp and to install it on the Cloud Volumes ONTAP system.

Learn how to add NetApp Support Site accounts to Cloud Manager.

If Cloud Manager can't access the license file over the secure internet connection, you can obtain the file yourself and then manually upload the file to Cloud Manager.

License expiration

Cloud Manager displays a warning 30 days before a node-based license is due to expire and again when the license expires. The following image shows a 30-day expiration warning that appears in the user interface:

You can select the working environment to review the message.

Cloud Manager includes a license expiration warning in the Cloud Volumes ONTAP report that's emailed to you, if you are an Account Admin and you enabled the option:

The emailed report includes the license expiration warning every 2 weeks.

If you don't renew the license in time, the Cloud Volumes ONTAP system shuts itself down. If you restart it, it shuts itself down again.

License renewal

When you renew a node-based BYOL subscription by contacting a NetApp representative, Cloud Manager automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system.

If Cloud Manager can't access the license file over the secure internet connection, you can obtain the file yourself and then manually upload the file to Cloud Manager.

License transfer to a new system

A node-based BYOL license is transferable between Cloud Volumes ONTAP systems when you delete an existing system and then create a new one using the same license.

For example, you might want to delete an existing licensed system and then use the license with a new BYOL system in a different VPC/VNet or cloud provider. Note that only *cloud-agnostic* serial numbers work in any cloud provider. Cloud-agnostic serial numbers start with the *908xxxx* prefix.

It's important to note that your BYOL license is tied to your company and a specific set of NetApp Support Site credentials.

AutoSupport and Active IQ Digital Advisor

The AutoSupport component of ONTAP collects telemetry and sends it for analysis. Active IQ Digital Advisor analyzes the data from AutoSupport and provides proactive care and optimization. Using artificial intelligence, Active IQ can identify potential problems and help you resolve them before they impact your business.

Active IQ enables you to optimize your data infrastructure across your global hybrid cloud by delivering actionable predictive analytics and proactive support through a cloud-based portal and mobile app. Data-driven insights and recommendations from Active IQ are available to all NetApp customers with an active SupportEdge contract (features vary by product and support tier).

Here are some things you can do with Active IQ:

- Plan upgrades.

  Active IQ identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP and the Upgrade Advisor component helps you plan for a successful upgrade.

- View system wellness.

  Your Active IQ dashboard reports any issues with wellness and helps you correct those issues. Monitor system capacity to make sure you never run out of storage space. View support cases for your system.

- Manage performance.

  Active IQ shows system performance over a longer period than you can see in ONTAP System Manager. Identify configuration and system issues that are impacting your performance.
  Maximize efficiency. View storage efficiency metrics and identify ways to store more data in less space.

- View inventory and configuration.

  Active IQ displays complete inventory and software and hardware configuration information. See when service contracts are expiring and renew them to ensure you remain supported.

Related information

- NetApp Documentation: Active IQ Digital Advisor
- Launch Active IQ
- SupportEdge Services

Default configuration for Cloud Volumes ONTAP

Understanding how Cloud Volumes ONTAP is configured by default can help you set up and administer your systems, especially if you are familiar with ONTAP because the

default setup for Cloud Volumes ONTAP is different than ONTAP.

Default setup

- Cloud Manager creates one data-serving storage VM when it deploys Cloud Volumes ONTAP. Some configurations support additional storage VMs. Learn more about managing storage VMs.

  Starting with the Cloud Manager 3.9.5 release, logical space reporting is enabled on the initial storage VM. When space is reported logically, ONTAP reports the volume space such that all the physical space saved by the storage efficiency features are also reported as used.

- Cloud Manager automatically installs the following ONTAP feature licenses on Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - Multi-tenant Encryption Key Management (MTEKM), starting with Cloud Volumes ONTAP 9.11.1
  - NetApp Volume Encryption (only for BYOL or registered PAYGO systems)
  - NFS
  - ONTAP S3

    Starting with Cloud Volumes ONTAP 9.9.1 in Azure

  - SnapMirror
  - SnapRestore
  - SnapVault

- Several network interfaces are created by default:
  - A cluster management LIF
  - An intercluster LIF
  - An SVM management LIF on HA systems in Azure
  - A node management LIF
  - An iSCSI data LIF
  - A CIFS and NFS data LIF

    > ⓘ LIF failover is disabled by default for Cloud Volumes ONTAP due to cloud provider requirements. Migrating a LIF to a different port breaks the external mapping between IP addresses and network interfaces on the instance, making the LIF inaccessible.

- Cloud Volumes ONTAP sends configuration backups to the Connector using HTTPS.

  The backups are accessible from https://ipaddress/occm/offboxconfig/ where *ipaddress* is the IP address of the Connector host.

- Cloud Manager sets a few volume attributes differently than other management tools (System Manager or the CLI, for example).

The following table lists the volume attributes that Cloud Manager sets differently from the defaults:

Attribute	Value set by Cloud Manager
Autosize mode	grow
Maximum autosize	1,000 percent ⓘ The Account Admin can modify this value from the Settings page.
Security style	NTFS for CIFS volumes UNIX for NFS volumes
Space guarantee style	none
UNIX permissions (NFS only)	777

See the *volume create* man page for information about these attributes.

Internal disks for system data

In addition to the storage for user data, Cloud Manager also purchases cloud storage for system data.

Azure (single node)

- Three Premium SSD disks:
    - One 10 GiB disk for boot data
    - One 140 GiB disk for root data
    - One 512 GiB disk for NVRAM

    If the virtual machine that you chose for Cloud Volumes ONTAP supports Ultra SSDs, then the system uses a 32 GiB Ultra SSD for NVRAM, rather than a Premium SSD.

- One 1024 GiB Standard HDD disk for saving cores
- One Azure snapshot for each boot disk and root disk
- Boot and root disks are encrypted by default.

Azure (HA pair)

- Two 10 GiB Premium SSD disks for the boot volume (one per node)
- Two 140 GiB Premium Storage page blobs for the root volume (one per node)
- Two 1024 GiB Standard HDD disks for saving cores (one per node)
- Two 512 GiB Premium SSD disks for NVRAM (one per node)
- One Azure snapshot for each boot disk and root disk
- Boot and root disks are encrypted by default.

Where the disks reside

Cloud Manager lays out the storage as follows:

- Boot data resides on a disk attached to the instance or virtual machine.

  This disk, which contains the boot image, is not available to Cloud Volumes ONTAP.

- Root data, which contains the system configuration and logs, resides in aggr0.
- The storage virtual machine (SVM) root volume resides in aggr1.
- Data volumes also reside in aggr1.

Knowledge and support

Register for support

Before you can open a support case with NetApp technical support, you need to add a NetApp Support Site (NSS) account to Cloud Manager and then register for support.

Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your Cloud Manager account ID support subscription (your 20 digit 960xxxxxxxxx serial number located on the Support Resources page in Cloud Manager).

  This serves as your single support subscription ID for any service within Cloud Manager. Each Cloud Manager account-level support subscription must be registered.

- Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider's marketplace (these are 20 digit 909201xxxxxxxx serial numbers).

  These serial numbers are commonly referred to as *PAYGO serial numbers* and get generated by Cloud Manager at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets, automatic case generation, and Active IQ.

How you register depends on whether you're a new or existing customer or partner.

- Existing customer or partner

  As an existing NetApp customer or partner, you can use your NetApp Support Site (NSS) SSO account to perform these registrations above. In the Support Dashboard, Cloud Manager provides an **NSS Management** page where you can add your NSS account. Once you add your NSS account, Cloud Manager automatically registers these serial numbers for you.

  Learn how to add your NSS account.

- New to NetApp

  If you're brand new to NetApp, you must complete a one-time registration of your Cloud Manager account ID serial number on NetApp's support registration site. Once you complete this registration and create a new NSS account, you can use this account in Cloud Manager to auto register going forward.

  Learn how to register with NetApp.

Add an NSS account to Cloud Manager

The Support Dashboard enables you to add and manage your NetApp Support Site accounts for use with Cloud Manager.

- If you have a customer-level account, you can add one or more NSS accounts.

- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added

alongside customer-level accounts.

Steps

1. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

2. Click **NSS Management > Add NSS Account**.

3. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

4. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

   These actions enable Cloud Manager to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

   Note the following:

   ◦ The account must be a customer-level account (not a guest or temp account).

   ◦ Upon successful login, NetApp will store the NSS user name. This is a system generated ID that maps to your email. On the **NSS Management** page, you can display your email from the ••• menu.

   ◦ If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the ••• menu. Using this option prompts you to log in again.

Register with NetApp

How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

Existing customer with an NSS account

If you're a NetApp customer with an NSS account, you simply need to register for support through Cloud Manager.

Steps

1. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

2. If you haven't already done so, add your NSS account to Cloud Manager.

3. On the **Resources** page, click **Register for Support**.
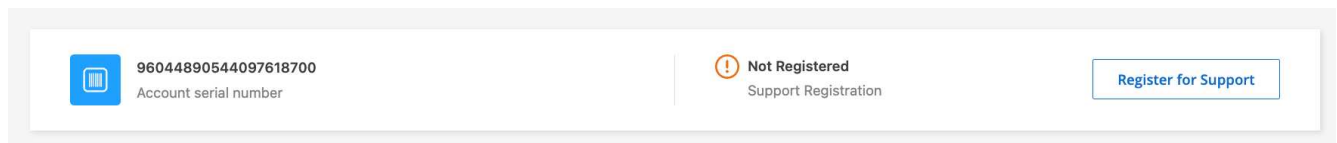
Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you just need to create an NSS account.

Steps

1. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form

   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.

   b. Be sure to copy the Cloud Manager Account Serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

Brand new to NetApp

If you are brand new to NetApp and you don't have an NSS account, follow each step below.

Steps

1. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

2. Locate your Cloud Manager account ID serial number from the Support Registration page.

3. Navigate to NetApp's support registration site and select **I am not a registered NetApp Customer**.

4. Fill out the mandatory fields (those with red asterisks).

5. In the **Product Line** field, select **Cloud Manager** and then select your applicable billing provider.

6. Copy your Cloud Manager account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

   An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn't arrive in few minutes.

7. Confirm the action from within the email.

   Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form

   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.

   b. Be sure to copy the Cloud Manager Account Serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, you can navigate to Cloud Manager to add this NSS account for future registrations.

Get help

NetApp provides support for Cloud Manager and its cloud services in a variety of ways. Extensive free self-

support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Self support

These options are available for free, 24 hours a day, 7 days a week:

- Knowledge base

  Search through the Cloud Manager knowledge base to find helpful articles to troubleshoot issues.

- Communities

  Join the Cloud Manager community to follow ongoing discussions or create new ones.

- Documentation

  The Cloud Manager documentation that you're currently viewing.

- Feedback email

  We value your input. Submit feedback to help us improve Cloud Manager.

NetApp support

In addition to the self-support options above, you can work with a NetApp Support specialist to resolve any issues after you activate support.

Before you get started

To use the **Create a Case** capability, you must first perform a one-time registration of your Cloud Manager Account ID serial number (ie. 960xxxx) with NetApp. Learn how to register for support.

Steps

1. In Cloud Manager, click **Help > Support**.

2. Choose one of the available options under Technical Support:

   a. Click **Call Us** if you'd like to speak with someone on the phone. You'll be directed to a page on netapp.com that lists the phone numbers that you can call.

   b. Click **Create a Case** to open a ticket with a NetApp Support specialists:

      - **NetApp Support Site Account**: Select the applicable NSS account associated with the person opening the support case. This person will be the primary contact for NetApp to reach out to, in addition to the additional emails provided below.

        If you don't see your NSS account, you can navigate to the **NSS Management** tab within Support section of Cloud Manager to add it there.

      - **Service**: Select the service that the issue is associated with. For example, Cloud Manager when specific to a technical support issue with workflows or functionality within the service.

      - **Working Environment**: If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.

        The list of working environments are within scope of the Cloud Manager Account, Workspace, and Connector you have selected in the top banner of the service.

▪ **Case Priority**: Choose the priority for the case, which can be Low, Medium, High, or Critical.

To learn more details about these priorities, hover your mouse over the information icon next to the field name.

▪ **Issue Description**: Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

▪ **Additional Email Addresses**: Enter additional email addresses if you'd like to make someone else aware of this issue.

Create a Case

TESTCLOUD2NTAP ✎

NetApp Support Site Account

Service

| Cloud Manager | ⌄ |

Working Environment

| Select... | ⌄ |

Case Priority ⓘ

| Low- General Guidance | ⌄ |

Issue Description

Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

Additional Email Addresses (Optional) ⓘ

Attachment (Optional) **Coming Soon**

No files selected ⬆

After you finish

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.

For a history of your support cases, you can click **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It's possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it's associated with is not the same company of record for the Cloud Manager Account serial number (ie. 960xxxx) or the working environment serial number. You can check your list of NSS accounts at the top of the **Create a Case** form to find the right match, or you can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at https://mysupport.netapp.com/site/help

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- Notice for Cloud Manager
- Notices for the Cloud Volumes ONTAP mediator
- Notice for ONTAP