Cloud Volumes ONTAP documentation

Cloud Volumes ONTAP

NetApp
February 27, 2026

Table of Contents

Cloud Volumes ONTAP documentation . . . 1
Release notes . . . 2
What's new in Cloud Volumes ONTAP . . . 2
26 February 2026 . . . 2
19 February 2026 . . . 4
17 February 2026 . . . 4
12 February 2026 . . . 5
10 February 2026 . . . 5
9 February 2026 . . . 5
12 January 2026 . . . 8
10 December 2025 . . . 8
10 November 2025 . . . 8
17 October 2025 . . . 9
06 October 2025 . . . 9
04 September 2025 . . . 9
11 August 2025 . . . 9
14 July 2025 . . . 10
25 June 2025 . . . 10
29 May 2025 . . . 11
12 May 2025 . . . 11
16 April 2025 . . . 11
14 April 2025 . . . 11
03 April 2025 . . . 11
28 March 2025 . . . 12
12 March 2025 . . . 12
10 March 2025 . . . 12
06 March 2025 . . . 12
03 March 2025 . . . 12
18 February 2025 . . . 13
10 February 2025 . . . 13
09 December 2024 . . . 13
11 November 2024 . . . 14
25 October 2024 . . . 15
07 October 2024 . . . 15
09 September 2024 . . . 15
23 August 2024 . . . 16
22 August 2024 . . . 16
08 August 2024 . . . 16
10 June 2024 . . . 17
17 May 2024 . . . 17
23 April 2024 . . . 17
08 March 2024 . . . 18
05 March 2024 . . . 18

02 February 2024 . . . 18
16 January 2024 . . . 18
08 January 2024 . . . 18
06 December 2023 . . . 19
05 December 2023 . . . 19
10 November 2023 . . . 20
08 November 2023 . . . 20
01 November 2023 . . . 20
23 October 2023 . . . 20
06 October 2023 . . . 21
10 September 2023 . . . 21
30 July 2023 . . . 21
26 July 2023 . . . 22
02 July 2023 . . . 22
26 June 2023 . . . 22
04 June 2023 . . . 22
07 May 2023 . . . 23
04 April 2023 . . . 24
3 April 2023 . . . 24
13 March 2023 . . . 25
05 March 2023 . . . 25
05 February 2023 . . . 26
1 January 2023 . . . 27
15 December 2022 . . . 27
08 December 2022 . . . 27
04 December 2022 . . . 27
15 November 2022 . . . 28
06 November 2022 . . . 28
18 September 2022 . . . 28
31 July 2022 . . . 29
18 July 2022 . . . 30
3 July 2022 . . . 30
07 June 2022 . . . 31
02 May 2022 . . . 32
3 April 2022 . . . 34
27 February 2022 . . . 34
09 February 2022 . . . 34
06 February 2022 . . . 35
30 January 2022 . . . 35
02 January 2022 . . . 35
28 November 2021 . . . 37
04 October 2021 . . . 38
02 September 2021 . . . 38
07 July 2021 . . . 39
30 May 2021 . . . 41

24 May 2021 . . . 42
11 Apr 2021 . . . 42
08 Mar 2021 . . . 42
04 January 2021 . . . 43
03 Nov 2020 . . . 45
Known limitations . . . 45
Console doesn’t support FlexGroup volumes creation . . . 45
Console doesn’t support S3 with Cloud Volumes ONTAP . . . 45
Console doesn’t support disaster recovery for storage VMs . . . 45
Cloud Volumes ONTAP Release Notes . . . 45
Get started . . . 47
Learn about Cloud Volumes ONTAP . . . 47
Supported ONTAP versions for Cloud Volumes ONTAP deployments . . . 48
AWS . . . 48
Azure . . . 49
Google Cloud . . . 49
Get started in Amazon Web Services . . . 50
Quick start for Cloud Volumes ONTAP in AWS . . . 50
Plan your Cloud Volumes ONTAP configuration in AWS . . . 52
Set up your networking . . . 56
Set up Cloud Volumes ONTAP to use a customer-managed key in AWS . . . 79
Set up AWS IAM roles for Cloud Volumes ONTAP nodes . . . 82
Set up licensing for Cloud Volumes ONTAP in AWS . . . 91
Deploy Cloud Volumes ONTAP in AWS using quick deployment . . . 99
Launch Cloud Volumes ONTAP in AWS . . . 102
Deploy Cloud Volumes ONTAP in AWS Secret Cloud or AWS Top Secret Cloud . . . 115
Get started in Microsoft Azure . . . 131
Learn about Cloud Volumes ONTAP deployment options in Azure . . . 131
Get started in NetApp Console . . . 132
Deploy Cloud Volumes ONTAP from the Azure marketplace . . . 183
Get started in Google Cloud . . . 187
Quick start for Cloud Volumes ONTAP in Google Cloud . . . 187
Plan your Cloud Volumes ONTAP configuration in Google Cloud . . . 188
Set up Google Cloud networking for Cloud Volumes ONTAP . . . 191
Set up VPC Service Controls to deploy Cloud Volumes ONTAP in Google Cloud . . . 202
Create a Google Cloud service account for Cloud Volumes ONTAP . . . 205
Using customer-managed encryption keys with Cloud Volumes ONTAP . . . 208
Set up licensing for Cloud Volumes ONTAP in Google Cloud . . . 209
Launch Cloud Volumes ONTAP in Google Cloud . . . 214
Google Cloud Platform Image Verification . . . 227
Use Cloud Volumes ONTAP . . . 239
License management . . . 239
Manage capacity-based licensing for Cloud Volumes ONTAP . . . 239
Manage Keystone subscriptions for Cloud Volumes ONTAP through NetApp Console . . . 244
Manage node-based licensing for Cloud Volumes ONTAP . . . 246

Volume and LUN administration . . . 251
Create a FlexVol volume on a Cloud Volumes ONTAP system . . . 251
Manage volumes on Cloud Volumes ONTAP systems . . . 258
Tier inactive Cloud Volumes ONTAP data to a low-cost object storage . . . 267
Connect to a LUN on Cloud Volumes ONTAP from your host system . . . 274
Accelerate data access with FlexCache volumes on a Cloud Volumes ONTAP system . . . 275
Aggregate administration . . . 276
Create an aggregate for Cloud Volumes ONTAP systems . . . 276
Manage aggregates for Cloud Volumes ONTAP clusters . . . 279
Manage the Cloud Volumes ONTAP aggregate capacity on a Console agent . . . 280
Manage disk performance in Azure . . . 282
Storage VM administration . . . 285
Manage storage VMs for Cloud Volumes ONTAP . . . 285
Manage data-serving storage VMs for Cloud Volumes ONTAP in AWS . . . 286
Manage data-serving storage VMs for Cloud Volumes ONTAP in Azure . . . 293
Manage data-serving storage VMs for Cloud Volumes ONTAP in Google Cloud . . . 296
Set up storage VM disaster recovery for Cloud Volumes ONTAP . . . 299
Security and data encryption . . . 299
Encrypt volumes on Cloud Volumes ONTAP with NetApp encryption solutions . . . 299
Manage Cloud Volumes ONTAP encryption keys with AWS Key Management Service . . . 300
Manage Cloud Volumes ONTAP encryption keys with Azure Key Vault . . . 301
Manage Cloud Volumes ONTAP encryption keys with Google Cloud KMS . . . 308
Enable NetApp ransomware protection solutions for Cloud Volumes ONTAP . . . 310
Create tamperproof Snapshot copies of WORM files on Cloud Volumes ONTAP . . . 313
System administration . . . 314
Upgrade Cloud Volumes ONTAP . . . 314
Register Cloud Volumes ONTAP pay-as-you-go systems . . . 324
Convert a Cloud Volumes ONTAP node-based license to a capacity-based license . . . 325
Start and stop a Cloud Volumes ONTAP system . . . 328
Synchronize Cloud Volumes ONTAP system time using the NTP server . . . 330
Modify system write speed . . . 331
Change the Cloud Volumes ONTAP cluster admin password . . . 331
Add, remove, or delete systems . . . 332
AWS administration . . . 334
Azure administration . . . 336
Google Cloud administration . . . 348
Administer Cloud Volumes ONTAP using System Manager . . . 356
Administer Cloud Volumes ONTAP from the CLI . . . 359
System health and events . . . 359
Verify AutoSupport setup for Cloud Volumes ONTAP . . . 359
Configure EMS for Cloud Volumes ONTAP systems . . . 363
Concepts . . . 364
Licensing . . . 364
Licensing for Cloud Volumes ONTAP . . . 364
Learn more about capacity-based licenses for Cloud Volumes ONTAP . . . 368

Storage . . . 372
Supported client protocols for Cloud Volumes ONTAP . . . 372
Disks and aggregates used for Cloud Volumes ONTAP clusters . . . 373
Learn about support for AWS Elastic Volumes with Cloud Volumes ONTAP . . . 376
Learn about data tiering with Cloud Volumes ONTAP in AWS, Azure, or Google Cloud . . . 382
Cloud Volumes ONTAP storage management . . . 387
Write speed . . . 389
Flash Cache . . . 392
Learn about WORM storage on Cloud Volumes ONTAP . . . 392
High-availability pairs . . . 394
Learn about Cloud Volumes ONTAP HA pairs in AWS . . . 395
Learn about Cloud Volumes ONTAP HA pairs in Azure . . . 401
Learn about Cloud Volumes ONTAP HA pairs in Google Cloud . . . 407
Operations unavailable when a node in Cloud Volumes ONTAP HA pair is offline . . . 411
Learn about Cloud Volumes ONTAP data encryption and ransomware protection . . . 412
Encryption of data at rest . . . 412
ONTAP virus scanning . . . 413
Ransomware protection . . . 413
Learn about performance monitoring for Cloud Volumes ONTAP workloads . . . 414
Performance technical reports . . . 414
CPU performance . . . 414
License management for node-based BYOL . . . 415
BYOL system licenses . . . 415
License management for a new system . . . 415
License expiration . . . 415
License renewal . . . 416
License transfer to a new system . . . 416
Learn how AutoSupport and Digital Advisor are used for Cloud Volumes ONTAP . . . 416
Supported default configurations for Cloud Volumes ONTAP . . . 417
Default setup . . . 417
Internal disks for system data . . . 419
Knowledge and support . . . 423
Register for support . . . 423
Support registration overview . . . 423
Register NetApp Console for NetApp support . . . 423
Associate NSS credentials for Cloud Volumes ONTAP support . . . 425
Get help . . . 427
Get support for a cloud provider file service . . . 427
Use self-support options . . . 427
Create a case with NetApp support . . . 427
Manage your support cases . . . 429
Legal notices . . . 431
Copyright . . . 431
Trademarks . . . 431
Patents . . . 431

Privacy policy 431
Open source 431

Cloud Volumes ONTAP documentation

Release notes

What's new in Cloud Volumes ONTAP

Learn what's new with Cloud Volumes ONTAP management in the NetApp Console.

The enhancements described on this page are specific to managing Cloud Volumes ONTAP through the Console. To learn what's new with the Cloud Volumes ONTAP software itself, go to the Cloud Volumes ONTAP Release Notes.

26 February 2026

Support for Google Infrastructure Manager for private mode deployments

Cloud Volumes ONTAP 9.16.1 and later now support Google Cloud Infrastructure Manager (IM) instead of Cloud Deployment Manager (DM) for new private mode deployments in Google Cloud. Google will deprecate Deployment Manager as an infrastructure service in the near future for the more advanced Infrastructure Manager.

Beginning February 25, 2026, Cloud Volumes ONTAP uses Infrastructure Manager for new and existing private mode deployments. This table explains the basic workflows for you:

Scenario	Action	New APIs for the agent	New permissions for the agent	New Google Cloud APIs for Cloud Volumes ONTAP	Doc resources
Existing agent and existing deployment in private mode	Upgrade to the latest version of NetApp Console agent by downloading the installer from the NetApp Support Site and then manually installing the agent on your host, so that it can use Infrastructure Manager APIs. Thereafter, convert the existing Cloud Volumes ONTAP systems to use Infrastructure Manager.	• Cloud Infrastructure Manager API • Cloud Quotas API • Cloud Build API	All the permissions listed for the Console release on: • 8 December 2025 • 09 February 2026 • cloudbuild.workerpools.get • cloudbuild.workerpools.get	• https://cloudbuild.googleapis.com/v1 • https://www.googleapis.com/upload/storage/v1 • https://config.googleapis.com/v1	Configure existing Cloud Volumes ONTAP deployments for Google Cloud Infrastructure Manager
New agent and new deployment	Create a new agent and deploy a new Cloud Volumes ONTAP system in private mode.				• Create a Console agent from Google Cloud • Quick start for private mode deployments

In private mode deployments, you need a few configuration changes for Cloud Volumes ONTAP to start using Infrastructure Manager. Refer to Infrastructure Manager configuration for private mode deployments.

Related links

- NetApp Console Agent 4.2.0 Release Notes
- Permissions required for Google Cloud Infrastructure Manager

19 February 2026

New regions supported in Azure

You can now deploy Cloud Volumes ONTAP 9.12.1 GA and later in single and multiple availability zones in Azure in the following regions. This includes support for both single-node and high-availability (HA) deployments.

- Japan West (japanwest)
- Indonesia Central (indonesiacentral)

For a list of all regions, refer to the Global Regions Map under Azure.

17 February 2026

Cloud Volumes ONTAP support for next generation Google Cloud VMs

With 9.18.1, NetApp transitions new Cloud Volumes ONTAP deployments off N2 VMs to the next generation Google Cloud C3 series VMs for a faster and more scalable experience. You can now take advantage of C3 series VMs while deploying Cloud Volumes ONTAP 9.18.1 and later in Google Cloud. The C3 series machines offer improved performance and higher capacity limits by using Google Virtual NIC (gVNIC) and Hyperdisk Balanced disks that ensure dynamic performance for intensive workloads.

> For now, Cloud Volumes ONTAP supports the C3 series only in single-node deployments.

If your Cloud Volumes ONTAP system runs 9.18.1 or later, the preconfigured packages that you use for easy single node deployments automatically use C3 VMs, while enabling you to customize the IOPS and throughput parameters based on your workload needs. Similarly, while creating aggregates, you can add Hyperdisk Balanced disks to achieve better performance and scalability in Google Cloud. Additionally, you can select the LSSD variants of the C3 series machines for default Flash Cache support.

You can’t change the disk type for C3 VMs when adding volumes to aggregates because C3 supports only Hyperdisk Balanced disks. Similarly, when replicating a system with N2 VM types to a C3 VM, the disk type is set by default to Hyperdisk Balanced.

Supported configurations for Cloud Volumes ONTAP in Google Cloud

Google documents: C3 machine series

VNet security for Cloud Volumes ONTAP in Azure

Cloud Volumes ONTAP 9.18.1 and later deployments in Azure single and multiple availability zones support Azure Virtual Network (VNet) encryption as part of its layered security strategy to protect data in transit. Cloud Volumes ONTAP leverages Azure’s native Datagram Transport Layer Security (DTLS) protocol to secure communication between ONTAP nodes, management interfaces, and other Azure services, preventing interception and unauthorized access. This network-level encryption complements ONTAP's built-in storage and data-at-rest protections to deliver end-to-end security of your data.

Networking for Azure VNet encryption

12 February 2026

Support for Ebdsv5 and E104ids_v5 VMs in Azure

Beginning with Cloud Volumes ONTAP 9.18.1, you can deploy Ebdsv5 and E104ids_v5 VMs for single-node and high-availability (HA) deployments and upgrades.

Ebdsv5 VMs within the Eb family of Azure virtual machines are optimized for higher remote storage performance. You can use these VMs for memory-intensive and I/O-heavy enterprise workloads, such as relational databases, in-memory analytics, and other demanding business-critical applications.

E104ids_v5 is an isolated VM instance that helps you better handle scheduled maintenance windows. Compared to E80ids_v4, it offers much higher disk throughput and IOPS, along with better overall network performance.

Supported configurations for Cloud Volumes ONTAP in Azure

Azure documentation: Edsv5 sizes series

10 February 2026

Cloud Volumes ONTAP 9.18.1 GA

You can now use the NetApp Console to deploy and manage the General Availability (GA) version of Cloud Volumes ONTAP 9.18.1 in AWS, Azure, and Google Cloud.

Learn more about this release of Cloud Volumes ONTAP.

9 February 2026

Support for Google Cloud Infrastructure Manager

Cloud Volumes ONTAP 9.16.1 and later now support Google Cloud Infrastructure Manager (IM) instead of Cloud Deployment Manager (DM) for new deployments in Google Cloud. Google will deprecate Deployment Manager as an infrastructure service in the near future for the more advanced Infrastructure Manager.

Beginning February 09, 2026, Cloud Volumes ONTAP uses Infrastructure Manager for new and existing deployments. This table explains a few workflows for you:

Scenario	Action	New APIs for the agent	New permissions for the agent	New Google Cloud APIs for Cloud Volumes ONTAP	Doc resources
Existing agent and existing Cloud Volumes ONTAP deployment	Add new APIs and permissions to the existing agent and convert the existing Cloud Volumes ONTAP system.	• Cloud Infrastructure Manager API • Cloud Quotas API	All the permissions listed for the Console release on: • 8 December 2025 • 09 February 2026	https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1	Configure existing Cloud Volumes ONTAP deployments for Google Cloud Infrastructure Manager
Existing agent and new Cloud Volumes ONTAP deployment	Add new APIs and permissions to the existing agent and deploy a new Cloud Volumes ONTAP system.	• Cloud Infrastructure Manager API • Cloud Quotas API	All the permissions listed for the Console release on: • 8 December 2025 • 09 February 2026	All the steps for new deployment	Getting started with Cloud Volumes ONTAP in Google Cloud

Scenario	Action	New APIs for the agent	New permissions for the agent	New Google Cloud APIs for Cloud Volumes ONTAP	Doc resources
New agent and new deployment	Create a new agent and deploy a new Cloud Volumes ONTAP system.				• Create a Console agent from Google Cloud • Getting started with Cloud Volumes ONTAP in Google Cloud

Now, deploy Cloud Volumes ONTAP to automatically use Infrastructure Manager or switch your existing deployments in Deployment Manager to Infrastructure Manager by running a conversion tool. The conversion is a one-time process, after which your systems will start using Infrastructure Manager. Refer to Configure existing Cloud Volumes ONTAP deployments for Google Cloud Infrastructure Manager for instructions on running the conversion tool.

Cloud Volumes ONTAP systems that use Infrastructure Manager use Google Cloud Storage buckets to store data and records in the zone of the first deployment to store deployment records, which are reused for subsequent deployments. You might incur extra costs for these buckets, but do not edit or delete the buckets or their content:

- `gs://netapp-cvo-infrastructure-manager-<project id>`: for ONTAP versions and SVM Terraform Templates used for new Cloud Volumes ONTAP deployments. Inside this, the `dm-to-im-convert` bucket contains the Cloud Volumes ONTAP Terraform files.
- `<gcp project number>-<region>-blueprint-config`: for storing Google Cloud Terraform artifacts.

Related links

- Getting started with Cloud Volumes ONTAP in Google Cloud
- NetApp Console Agent 4.2.0 Release Notes
- Permissions required for Google Cloud Infrastructure Manager

12 January 2026

Preferred billing option for Cloud Volumes ONTAP

You can now select a preferred billing option for calculating your Cloud Volumes ONTAP usage and overages. Since the limited availability of the Bring Your Own Licenses (BYOL) licensing model on June 25, 2025, NetApp has added preferred charging methods in the **Licensing and Subscriptions** section of the NetApp Console. You can use either your annual marketplace subscription for billing and overages or the existing BYOL model as the preferred option. This gives you the flexibility to choose the charging method that best fits your organization's financial strategy and usage patterns.

Billing preferences and overages.

10 December 2025

Ability to enhance performance of Premium SSD v2 disks in Azure

You can now enhance the performance of Premium SSD v2 Managed Disks in Azure by modifying the IOPS and throughput parameters. Using this capability, you can optimize the storage performance of your systems based on your workload requirements.

Manage Premium SSD v2 disk performance for Cloud Volumes ONTAP in Azure.

Overage charging for Essentials licenses simplified

For Cloud Volumes ONTAP marketplace annual contracts/private offers, overage calculations for Essentials licenses is now aligned with Bring Your Own License (BYOL) packages. Previously, overages were billed at hourly marketplace rates for the exact Essentials package. Now, if your marketplace annual contract includes multiple Essentials packages, the NetApp Console charges overages for an Essentials package against the available capacity of a higher-priced Essentials package in your subscription. This simplifies overage calculations for Essentials packages and ensures a smooth transition from BYOL licensing to a subscription-based model.

How overages are charged for Essentials licenses

Support for Azure Edsv6 sizes series

Beginning with Cloud Volumes ONTAP 9.17.1, you can deploy Azure Edsv6 series VMs through the NetApp Console for new Cloud Volumes ONTAP instances. Cloud Volumes ONTAP 9.17.1 and later will support only Generation 2 VMs for new deployments. These Generation 2 machines are compatible with the latest technologies, such as Unified Extensible Firmware Interface (UEFI), Azure Boost systems, and NVMe. They are ideal for memory-intensive systems and applications that need fast, local storage, such as database servers and analytics engines.

Supported configurations for Cloud Volumes ONTAP in Azure

10 November 2025

Enhanced NVMe-TCP Support

Earlier, when deploying Cloud Volumes ONTAP instances over NVMe-TCP, you would have to to manually obtain and apply NVMe licenses before deployment. With this update, Cloud Volumes ONTAP now automatically installs the required NVMe licenses during deployment, simplifying the setup process.

For existing NVMe-TCP deployments that lack licenses, Cloud Volumes ONTAP applies the licenses automatically. You must restart the system for the licenses to take effect.

For more information, see Supported client protocols for Cloud Volumes ONTAP: NVMe-TCP.

17 October 2025

Cloud Volumes ONTAP in Azure now limited to latest supported versions

Cloud Volumes ONTAP deployments and upgrades in Azure through the NetApp Console are now restricted to the latest supported versions. This ensures compatibility with the latest generation hardware supported by Microsoft and provides the newest features and security enhancements. The Console will prompt you to upgrade to the supported versions.

For more details, refer to:

- Deployment: Supported ONTAP versions for Cloud Volumes ONTAP deployments
- Upgrade: Supported upgrade paths for Azure

06 October 2025

BlueXP is now NetApp Console

The NetApp Console, built on the enhanced and restructured BlueXP foundation, provides centralized management of NetApp storage and NetApp Data Services across on-premises and cloud environments at enterprise grade—delivering real-time insights, faster workflows, and simplified administration, that is highly secure and compliant.

For details on what has changed, see the NetApp Console release notes.

Simplified Cloud Volumes ONTAP deployment in AWS

You can now deploy Cloud Volumes ONTAP in AWS using a quick deployment method for both single-node and high-availability (HA) configurations. This streamlined process reduces the number of steps compared to the advanced method, automatically sets default values on a single page, and minimizes navigation, making deployment faster and easier.

For more information, refer to Deploy Cloud Volumes ONTAP in AWS using quick deployment.

04 September 2025

Cloud Volumes ONTAP 9.17.1 RC

You can now use BlueXP to deploy and manage the Release Candidate 1 of Cloud Volumes ONTAP 9.17.1 in Azure and Google Cloud. However, this version is not available for deployment and upgrade in AWS.

Learn more about this release of Cloud Volumes ONTAP.

11 August 2025

End of availability of Optimized licenses

Beginning on August 11, 2025, the Cloud Volumes ONTAP Optimized license will be deprecated and will no longer be available for purchase or renewal in the Azure and Google Cloud marketplaces for pay-as-you-go (PAYGO) subscriptions. If you have an existing annual contract with an Optimized license, you can continue to use the license until the end of your contract. When your Optimized license expires, you can opt for Cloud Volumes ONTAP Essentials or Professional licenses in BlueXP.

However, the ability to add or renew Optimized licenses will be available through the APIs.

For information about licensing packages, refer to Licensing for Cloud Volumes ONTAP.

For information about switching to a different charging method, refer to Manage capacity-based licensing.

14 July 2025

Support for transparent proxy

BlueXP now supports transparent proxy servers in addition to the existing explicit proxy connections. When creating or modifying the BlueXP Connector, you can configure a transparent proxy server to securely manage network traffic to and from Cloud Volumes ONTAP.

For more information about the use of proxy servers in Cloud Volumes ONTAP, refer to:

- Network configurations to support Connector proxy in AWS
- Network configurations to support Connector proxy in Azure
- Network configurations to support Connector proxy in Google Cloud

New VM type supported for Cloud Volumes ONTAP in Azure

Beginning with Cloud Volumes ONTAP 9.13.1, L8s_v3 is supported as a VM type in Azure single and multiple availability zones, for both new and existing high-availability (HA) pair deployments.

For more information, refer to
Supported configurations in Azure.

25 June 2025

Restricted availability of BYOL licensing for Cloud Volumes ONTAP

Beginning June 25, 2025, NetApp has restricted the bring your own license (BYOL) licensing model for Cloud Volumes ONTAP. The restriction applies to all customers and Cloud Volumes ONTAP deployments in AWS, Azure, and Google Cloud. The only exemptions are the U.S. Public Sector customers and China region deployments.

NetApp support and services will continue until your BYOL contract expires, but your expired licenses will not be renewed or extended. When your BYOL licenses expire, you must replace them with capacity-based licenses purchased through your cloud marketplace subscriptions. A capacity-based licensing model through hyperscaler marketplaces streamlines the licensing experience and delivers greater business benefits. Contact your NetApp accounts team or customer success representatives to discuss your options of conversion.

For more information, refer to this customer communiqué: CPC-00661: Changes to Cloud Volumes ONTAP BYOL Policy.

29 May 2025

Private mode deployments enabled for Cloud Volumes ONTAP 9.15.1

You can now deploy Cloud Volumes ONTAP 9.15.1 in private mode in AWS, Azure, and Google Cloud. Private mode is enabled for both single-node and high-availability (HA) deployments of Cloud Volumes ONTAP 9.15.1.

For more information about private mode deployments refer to
Learn about BlueXP deployment modes.

12 May 2025

Discovery of deployments made through the Azure marketplace in BlueXP

BlueXP now has the capability of discovering the Cloud Volumes ONTAP systems deployed directly through the Azure marketplace. This means that you can now add and manage these systems as working environments in BlueXP, just like any other Cloud Volumes ONTAP system.

Deploy Cloud Volumes ONTAP from the Azure marketplace

16 April 2025

New regions supported in Azure

You can now deploy Cloud Volumes ONTAP 9.12.1 GA and later in single and multiple availability zones in Azure in the following regions. This includes support for both single-node and high-availability (HA) deployments.

- Spain Central
- Mexico Central

For a list of all regions, refer to the Global Regions Map under Azure.

14 April 2025

Storage VM creation automated through the APIs in Google Cloud

You can now use the BlueXP APIs to automate the storage VM creation in Google Cloud. You have been using this feature in Cloud Volumes ONTAP high-availability (HA) configurations, and now you can also use it in single node deployments. By using the BlueXP APIs, you can easily create, rename, and delete additional data-serving storage VMs in your Google Cloud environment, without the need to manually configure the required network interfaces, LIFs, and management LIFs. This automation simplifies the process of managing storage VMs.

Manage data-serving storage VMs for Cloud Volumes ONTAP in Google Cloud

03 April 2025

Support for China regions for Cloud Volumes ONTAP 9.13.1 in AWS

You can now deploy Cloud Volumes ONTAP 9.13.1 in AWS in China regions. This includes support for both single-node and high-availability (HA) deployments. Only licenses purchased directly from NetApp are supported.

For regional availability, refer to the Global Regions Maps for Cloud Volumes ONTAP.

28 March 2025

Private mode deployments enabled for Cloud Volumes ONTAP 9.14.1

You can now deploy Cloud Volumes ONTAP 9.14.1 in private mode in AWS, Azure, and Google Cloud. Private mode is enabled for both single-node and high-availability (HA) deployments of Cloud Volumes ONTAP 9.14.1.

For more information about private mode deployments refer to Learn about BlueXP deployment modes.

12 March 2025

New regions supported for multiple availability zone deployments in Azure

The following regions now support HA multiple availability zone deployments in Azure for Cloud Volumes ONTAP 9.12.1 GA and later:

- Central US
- US Gov Virginia (US Government Region - Virginia)

For a list of all regions, refer to the Global Regions Map under Azure.

10 March 2025

Storage VM creation automated through the APIs in Azure

You can now use the BlueXP APIs to create, rename, and delete additional data-serving storage VMs for Cloud Volumes ONTAP in Azure. Using the APIs automates the process of storage VM creation, including the configuration of the required network interfaces, LIFs, and a management LIF, if you need to use a storage VM for management purposes.

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

06 March 2025

Cloud Volumes ONTAP 9.16.1 GA

You can now use BlueXP to deploy and manage the Cloud Volumes ONTAP 9.16.1 General Availability release in Azure and Google Cloud. However, this version is not available for deployment and upgrade in AWS.

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

03 March 2025

Support for New Zealand North region in Azure

The New Zealand North region is now supported in Azure for single node and high-availability (HA) configurations of Cloud Volumes ONTAP 9.12.1 GA and later. Note that the Lsv3 instance type is not supported in this region.

For a list of all supported regions, refer to the Global Regions Map under Azure.

18 February 2025

Introducing Azure marketplace direct deployment

You can now take advantage of Azure marketplace direct deployment to easily and quickly deploy Cloud Volumes ONTAP directly from the Azure marketplace. Using this streamlined method, you can explore the core features and capabilities of Cloud Volumes ONTAP in your environment without the need to set up the BlueXP Connector or meet other onboarding criteria required for deploying Cloud Volumes ONTAP through BlueXP.

- Learn about Cloud Volumes ONTAP deployment options in Azure
- Deploy Cloud Volumes ONTAP from the Azure marketplace

10 February 2025

User authentication enabled for accessing System Manager from BlueXP

As a BlueXP administrator, you can now activate authentication for ONTAP users accessing ONTAP System Manager from BlueXP. You can enable this option by editing the BlueXP Connector settings. This option is available for standard and private modes.

Administer Cloud Volumes ONTAP using System Manager.

BlueXP Advanced View renamed to System Manager

The option for advanced management of Cloud Volumes ONTAP from BlueXP through ONTAP System Manager has been renamed from **Advanced View** to **System Manager**.

Administer Cloud Volumes ONTAP using System Manager.

Introducing a simpler way to manage licenses with the BlueXP digital wallet

Now, you can experience simplified management of Cloud Volumes ONTAP licenses by using improved navigation points within the BlueXP digital wallet:

- Access your Cloud Volumes ONTAP license information easily through the **Administration > Licenses and subscriptions > Overview/Direct Licenses** tabs.
- Click **View** on the Cloud Volume ONTAP panel in the **Overview** tab to gain a comprehensive understanding of your capacity-based licenses. This advanced view offers detailed insight into your licenses and subscriptions.
- If you prefer the previous interface, you can click the **Switch to legacy view** button to view license details by type and modify charging methods for your licenses.

Manage capacity-based licenses.

09 December 2024

List of supported VMs updated for Azure to align with the best practices

The DS_v2 and Es_v3 machine families are no longer available for selection on BlueXP when deploying new instances of Cloud Volumes ONTAP in Azure. These families will be retained and supported only in older, existing systems. New deployments of Cloud Volumes ONTAP are supported in Azure only from the 9.12.1 release. We recommend that you switch to either Es_v4 or any other series compatible with Cloud Volumes ONTAP 9.12.1 and later. The DS_v2 and Es_v3 series machines, however, will be available for new deployments made through the API.

Supported configurations in Azure

11 November 2024

End of availability for node-based licenses

NetApp has planned the end of availability (EOA) and end of support (EOS) of Cloud Volumes ONTAP node-based licensing. Beginning with 11 November, 2024, the limited availability of node-based licenses has been terminated. The support for node-based licensing ends on 31 December, 2024. After the EOA of your node-based licenses, you should transition to capacity-based licensing by using the BlueXP license conversion tool.

For annual or longer-term commitments, NetApp recommends that you contact your NetApp representative prior to the EOA date or license expiration date to ensure that the prerequisites for the transition are in place. If you don't have a long-term contract for a Cloud Volumes ONTAP node and run your system against an on-demand pay-as-you-go (PAYGO) subscription, it is important to plan your conversion before the EOS date. For both long-term contracts and PAYGO subscriptions, you can use the BlueXP license conversion tool for a seamless conversion.

End of availability of node-based licenses
Convert a Cloud Volumes ONTAP node-based license to a capacity-based license

Removal of node-based deployments from BlueXP

The option to deploy Cloud Volumes ONTAP systems by using node-based licenses is deprecated on BlueXP. Except for a few special cases, you cannot use node-based licenses for Cloud Volumes ONTAP deployments for any cloud provider.

NetApp recognizes the following unique licensing requirements in compliance with contractual obligations and operational needs, and will continue to support node-based licenses in these situations:

- U.S. Public Sector customers
- Deployments in private mode
- China region deployments of Cloud Volumes ONTAP in AWS
- If you have a valid, non-expired by-node bring your own license (BYOL license)

End of availability of node-based licenses

Addition of a cold tier for Cloud Volumes ONTAP data on Azure Blob storage

BlueXP now enables you to select a cold tier to store the inactive capacity tier data on Azure Blob storage. Adding the cold tier to the existing hot and cool tiers provides you with a more affordable storage option and improved cost efficiency.

Data tiering in Azure

Option to restrict public access to storage account for Azure

You now have the option to restrict public access to your storage account for Cloud Volumes ONTAP systems in Azure. By disabling access, you can secure your private IP address from exposure even within the same VNet, should there be a need to comply with your organization's security policies. This option also disables data tiering for your Cloud Volumes ONTAP systems, and is applicable to both single node and high-availability pairs.

Security group rules.

WORM enablement after deploying Cloud Volumes ONTAP

You now have the ability to activate write once, read many (WORM) storage on an existing Cloud Volumes ONTAP system using BlueXP. This functionality provides you with the flexibility of enabling WORM on a working environment, even if WORM was not enabled on it during its creation. Once enabled, you cannot disable WORM.

Enabling WORM on a Cloud Volumes ONTAP working environment

25 October 2024

List of supported VMs updated for Google Cloud to align with the best practices

The n1 series machines are no longer available for selection on BlueXP when deploying new instances of Cloud Volumes ONTAP in Google Cloud. The n1 series machines will be retained and supported only in older, existing systems. New deployments of Cloud Volumes ONTAP are supported in Google Cloud only from the 9.8 release. We recommend that you switch to the n2 series machine types that are compatible with Cloud Volumes ONTAP 9.8 and later. The n1 series machines, however, will be available for new deployments performed through the API.

Supported configurations in Google Cloud.

Local Zones support for Amazon Web Services in private mode

BlueXP now supports AWS Local Zones for Cloud Volumes ONTAP high availability (HA) deployments in private mode. The support that was earlier limited to only standard mode has now been extended to include private mode.

> AWS Local Zones are not supported when using BlueXP in restricted mode.

For more information on AWS Local Zones with HA Deployments, refer to AWS Local Zones.

07 October 2024

Enhanced user experience in version selection for upgrade

Beginning with this release, when you try to upgrade Cloud Volumes ONTAP using the BlueXP notification, you will receive guidance on the default, latest, and compatible versions to use. Also, now you can select the latest patch or major version compatible with your Cloud Volumes ONTAP instance, or manually enter a version for upgrade.

Upgrade Cloud Volumes ONTAP software

09 September 2024

WORM and ARP functionalities are no longer chargeable

The built-in data protection and security features of WORM (Write Once Read Many) and ARP (Autonomous Ransomware Protection) will be offered with Cloud Volumes ONTAP licenses at no extra cost. The new pricing model applies to both new and existing BYOL and PAYGO/marketplace subscriptions of AWS, Azure, and Google Cloud. Both capacity-based and node-based licenses will contain ARP and WORM for all configurations, including single node and high-availability (HA) pairs, at no additional cost.

The simplified pricing brings you these benefits:

- Accounts that currently include WORM and ARP will no longer incur charges for these features. Going forward, your billing will only have charges for capacity usage, as it was before this change. WORM and ARP will no longer be included in your future bills.
- If your current accounts do not include these features, you can now opt for WORM and ARP at no additional cost.
- All Cloud Volumes ONTAP offerings for any new accounts will exclude charges for WORM and ARP.

Learn more about these features:

- Enable NetApp ransomware protection solutions for Cloud Volumes ONTAP
- WORM storage

23 August 2024

Canada West region now supported in AWS

The Canada West region is now supported in AWS for Cloud Volumes ONTAP 9.12.1 GA and later.

For a list of all regions, see the Global Regions Map under AWS.

22 August 2024

Cloud Volumes ONTAP 9.15.1 GA

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.15.1 General Availability release in AWS, Azure, and Google Cloud.

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

08 August 2024

Edge Cache licensing packages deprecated

Edge Cache capacity-based licensing packages will no longer be available for future deployments of Cloud Volumes ONTAP. However, you can use the API to avail this functionality.

Minimum version support for Flash Cache in Azure

The minimum Cloud Volumes ONTAP version required for configuring Flash Cache in Azure is 9.13.1 GA. You can only use ONTAP 9.13.1 GA and later versions for deploying Flash Cache on Cloud Volumes ONTAP systems in Azure.

For supported configurations, see Supported configurations in Azure.

Free trials for marketplace subscriptions deprecated

The 30-day automatic free trial or evaluation license for pay-as-you-go subscriptions in cloud provider's marketplace will no longer be available in Cloud Volumes ONTAP. The charging for any type of marketplace subscription (PAYGO or annual contract) will be activated from the first use, without any free trial period.

10 June 2024

Cloud Volumes ONTAP 9.15.0

BlueXP can now deploy and manage the Cloud Volumes ONTAP 9.15.0 in AWS, Azure, and Google Cloud.

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

17 May 2024

Amazon Web Services Local Zones support

Support for AWS Local Zones is now available for Cloud Volumes ONTAP HA deployments. AWS Local Zones are an infrastructure deployment where storage, compute, database, and other select AWS services are located close to large cities and industry areas.

> AWS Local Zones are supported when using BlueXP in standard mode. At this time, AWS Local Zones are not supported when using BlueXP in restricted mode or private mode.

For more information on AWS Local Zones with HA Deployments, refer to AWS Local Zones.

23 April 2024

New regions supported for multiple availability zone deployments in Azure

The following regions now support HA multiple availability zone deployments in Azure for Cloud Volumes ONTAP 9.12.1 GA and later:

- Germany West Central
- Poland Central
- West US 3
- Israel Central
- Italy North
- Canada Central

For a list of all regions, refer to the Global Regions Map under Azure.

Johannesburg region now supported in Google Cloud

The Johannesburg region (`africa-south1` region) is now supported in Google Cloud for Cloud Volumes ONTAP 9.12.1 GA and later.

For a list of all regions, refer to the Global Regions Map under Google Cloud.

Volume templates and tags no longer supported

You can no longer create a volume from a template or edit a volume's tags. These actions were associated with the BlueXP remediation service, which is no longer available.

08 March 2024

Amazon Instant Metadata Service v2 support

In AWS, Cloud Volumes ONTAP, the Mediator, and the Connector now support Amazon Instant Metadata Service v2 (IMDSv2) for all functions. IMDSv2 provides enhanced protection against vulnerabilities. Only IMDSv1 was previously supported.

If required by your security policies, you can configure your EC2 instances to use IMDSv2. For instructions, refer to BlueXP setup and administration documentation for managing existing Connectors.

05 March 2024

Cloud Volumes ONTAP 9.14.1 GA

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.14.1 General Availability release in AWS, Azure, and Google Cloud.

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

02 February 2024

Support for Edv5-series VMs in Azure

Cloud Volumes ONTAP now supports the following Edv5-series VMs starting with the 9.14.1 release.

- E4ds_v5
- E8ds_v5
- E20s_v5
- E32ds_v5
- E48ds_v5
- E64ds_v5

Supported configurations in Azure

16 January 2024

Patch releases in BlueXP

Patch releases are available in BlueXP only for the latest three versions of Cloud Volumes ONTAP.

Upgrade Cloud Volumes ONTAP

08 January 2024

New VMs for Azure multiple availability zones

Starting from Cloud Volumes ONTAP 9.13.1, the following VM types support Azure multiple availability zones for new and existing high-availability pair deployments:

- L16s_v3
- L32s_v3
- L48s_v3
- L64s_v3

Supported configurations in Azure

06 December 2023

Cloud Volumes ONTAP 9.14.1 RC1

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.14.1 in AWS, Azure, and Google Cloud.

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

300 TiB FlexVol volume max limit

You can now create a FlexVol volume up to the maximum size of 300 TiB with System Manager and the ONTAP CLI starting from Cloud Volumes ONTAP 9.12.1 P2 and 9.13.0 P2, and in BlueXP starting from Cloud Volumes ONTAP 9.13.1.

- Storage limits in AWS
- Storage limits in Azure
- Storage limits in Google Cloud

05 December 2023

The following changes were introduced.

New region support in Azure

Single availability zone region support

The following regions now support highly-available single availability zone deployments in Azure for Cloud Volumes ONTAP 9.12.1 GA and later:

- Tel Aviv
- Milan

Multiple availability zone region support

The following regions now support highly-available multiple availability zone deployments in Azure for Cloud Volumes ONTAP 9.12.1 GA and later:

- Central India
- Norway East
- Switzerland North

- South Africa North
- United Arab Emirates North

For a list of all regions, refer to the Global Regions Map under Azure.

10 November 2023

The following change was introduced with the 3.9.35 release of the Connector.

Berlin region now supported in Google Cloud

The Berlin region is now supported in Google Cloud for Cloud Volumes ONTAP 9.12.1 GA and later.

For a list of all regions, refer to the Global Regions Map under Google Cloud.

08 November 2023

The following change was introduced with the 3.9.35 release of the Connector.

Tel Aviv region now supported in AWS

The Tel Aviv region is now supported in AWS for Cloud Volumes ONTAP 9.12.1 GA and later.

For a list of all regions, refer to the Global Regions Map under AWS.

01 November 2023

The following change was introduced with the 3.9.34 release of the Connector.

Saudi Arabia region now supported in Google Cloud

The Saudi Arabia region is now supported in Google Cloud for Cloud Volumes ONTAP and the Connector for Cloud Volumes ONTAP 9.12.1 GA and later.

For a list of all regions, refer to the Global Regions Map under Google Cloud.

23 October 2023

The following change was introduced with the 3.9.34 release of the Connector.

New regions supported for HA multiple availability zone deployments in Azure

The following regions in Azure now support highly-available multiple availability zone deployments for Cloud Volumes ONTAP 9.12.1 GA and later:

- Australia East
- East Asia
- France Central
- North Europe
- Qatar Central
- Sweden Central

- West Europe
- West US 2

For a list of all regions that support multiple availability zones, refer to the Global Regions Map under Azure.

06 October 2023

The following change was introduced with the 3.9.34 release of the Connector.

Cloud Volumes ONTAP 9.14.0

BlueXP can now deploy and manage the Cloud Volumes ONTAP 9.14.0 General Availability release in AWS, Azure, and Google Cloud.

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

10 September 2023

The following change was introduced with the 3.9.33 release of the Connector.

Support for Lsv3-series VMs in Azure

The L48s_v3 and L64s_v3 instance types are now supported with Cloud Volumes ONTAP in Azure for single node and high-availability pair deployments with shared managed disks in single and multiple availability zones, starting with the 9.13.1 release. These instance types support Flash Cache.

View supported configurations for Cloud Volumes ONTAP in Azure
View storage limits for Cloud Volumes ONTAP in Azure

30 July 2023

The following changes were introduced with the 3.9.32 release of the Connector.

Flash Cache and high write speed support in Google Cloud

Flash Cache and high write speed can be enabled separately in Google Cloud for Cloud Volumes ONTAP 9.13.1 and later. High write speed is available on all supported instance types. Flash Cache is supported on the following instance types:

- n2-standard-16
- n2-standard-32
- n2-standard-48
- n2-standard-64

You can use these features separately or together on both single node and high-availability pair deployments.

Launch Cloud Volumes ONTAP in Google Cloud

Usage reports enhancements

Various improvements to the displayed information within the usage reports are now available. The following are enhancements to the usage reports:

- The TiB unit is now included in the name of columns.
- A new "node(s)" field for serial numbers is now included.
- A new “Workload Type” column is now included under the Storage VMs usage report.
- Working environment names now included in Storage VMs and Volume usage reports.
- Volume type “file” is now labeled “Primary (Read/Write)”.
- Volume type “secondary” is now labeled “Secondary (DP)”.

For more information on usage reports, refer to Download usage reports.

26 July 2023

The following changes were introduced with the 3.9.31 release of the Connector.

Cloud Volumes ONTAP 9.13.1 GA

BlueXP can now deploy and manage the Cloud Volumes ONTAP 9.13.1 General Availability release in AWS, Azure, and Google Cloud.

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

02 July 2023

The following changes were introduced with the 3.9.31 release of the Connector.

Support for HA multiple availability zone deployments in Azure

The Japan East and Korea Central in Azure now supports HA multiple availability zone deployments for Cloud Volumes ONTAP 9.12.1 GA and later.

For a list of all regions that support multiple availability zones, refer to the Global Regions Map under Azure.

Autonomous Ransomware Protection support

Autonomous Ransomware Protection (ARP) is now supported on Cloud Volumes ONTAP. ARP support is available on Cloud Volumes ONTAP version 9.12.1 and higher.

To learn more about ARP with Cloud Volumes ONTAP, refer to Autonomous Ransomware Protection.

26 June 2023

The following change was introduced with the 3.9.30 release of the Connector.

Cloud Volumes ONTAP 9.13.1 RC1

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.13.1 in AWS, Azure, and Google Cloud.

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

04 June 2023

The following change was introduced with the 3.9.30 release of the Connector.

Cloud Volumes ONTAP upgrade version selector update

Through the Upgrade Cloud Volumes ONTAP page, you can now choose to upgrade to the latest available version of Cloud Volumes ONTAP or an older version.

To learn more about upgrading Cloud Volumes ONTAP through BlueXP, refer to Upgrade Cloud Volumes ONTAP.

07 May 2023

The following changes were introduced with the 3.9.29 release of the Connector.

Qatar region now supported in Google Cloud

The Qatar region is now supported in Google Cloud for Cloud Volumes ONTAP and the Connector for Cloud Volumes ONTAP 9.12.1 GA and later.

Sweden Central region now supported in Azure

The Sweden Central region is now supported in Azure for Cloud Volumes ONTAP and the Connector for Cloud Volumes ONTAP 9.12.1 GA and later.

Support for HA multiple availability zone deployments in Azure Australia East

The Australia East region in Azure now supports HA multiple availability zone deployments for Cloud Volumes ONTAP 9.12.1 GA and later.

Charging usage breakdown

Now you can find out what you’re being charged for when you’re subscribed to capacity-based licenses. The following types of usage reports are available for download from the digital wallet in BlueXP. The usage reports provide capacity details of your subscriptions and tell you how you’re being charged for the resources in your Cloud Volumes ONTAP subscriptions. The downloadable reports can be easily shared with others.

- Cloud Volumes ONTAP package usage
- High-level usage
- Storage VMs usage
- Volumes usage

For more information, refer to Manage capacity-based licenses.

Notification now displays when accessing BlueXP without a marketplace subscription

A notification now displays whenever you access Cloud Volumes ONTAP in BlueXP without a marketplace subscription. The notification states "a marketplace subscription for this working environment is required to be compliant with Cloud Volumes ONTAP terms and conditions."

New permissions added to AWS IAM policy for HA mediators

These new AWS permissions have been added to the IAM policy for HA mediators in Cloud Volumes ONTAP high-availability (HA) environments:

- sts:AssumeRole

- ec2:DescribeSubnets

04 April 2023

Support for China regions for AWS

Starting with Cloud Volumes ONTAP 9.12.1 GA, China regions are now supported in AWS as follows.

- Single-node systems are supported.
- Licenses purchased directly from NetApp are supported.

For regional availability, refer to the Global Regions Maps for Cloud Volumes ONTAP.

3 April 2023

The following changes were introduced with the 3.9.28 release of the Connector.

Turin region now supported in Google Cloud

The Turin region is now supported in Google Cloud for Cloud Volumes ONTAP and the Connector for Cloud Volumes ONTAP 9.12.1 GA and later.

BlueXP digital wallet enhancement

The BlueXP digital wallet now shows the licensed capacity that you purchased with marketplace private offers.

Learn how to view the consumed capacity in your account.

Support for comments during volume creation

This release enables you to make comments when creating an Cloud Volumes ONTAP FlexGroup volume or FlexVol volume when using the API.

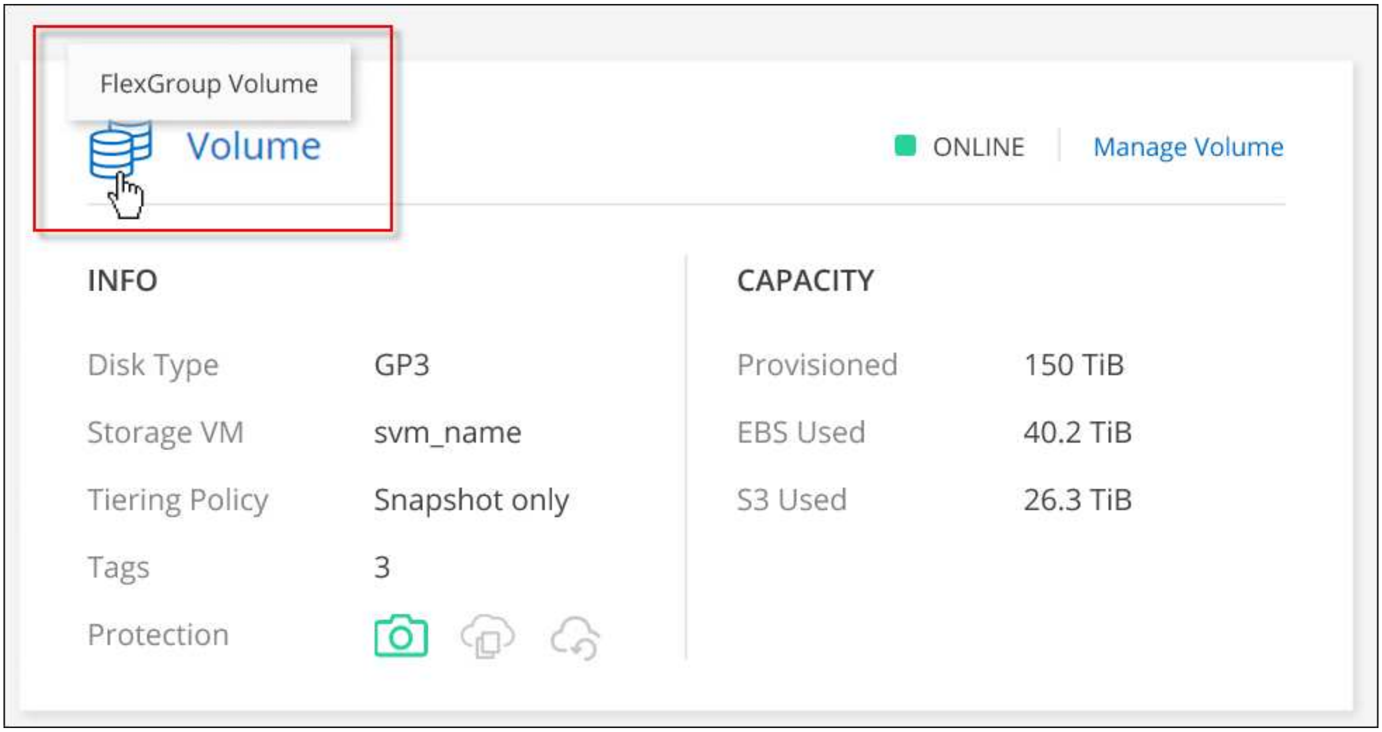
BlueXP user interface redesign for Cloud Volumes ONTAP Overview, Volumes, and Aggregates pages

BlueXP now has a redesigned user interface for Cloud Volumes ONTAP Overview, Volumes, and Aggregates pages. The tile-based design presents more comprehensive information in each tile for a better user experience.

FlexGroup Volumes viewable through Cloud Volumes ONTAP

FlexGroup volumes created through ONTAP System Manager or the ONTAP CLI directly are now viewable through the redesigned Volumes tile in BlueXP. Identical to the information provided for FlexVol volumes, BlueXP provides detailed information for created FlexGroup volumes through a dedicated Volumes tile.

> Currently, you can only view existing FlexGroup volumes under BlueXP. The ability to create FlexGroup volumes in BlueXP is not available but planned for a future release.



Learn more about viewing created FlexGroup volumes.

13 March 2023

Support for China regions in Azure

China North 3 region is now supported for single node deployments of Cloud Volumes ONTAP 9.12.1 GA and 9.13.0 GA in Azure. Only licenses purchased directly from NetApp (BYOL licenses) are supported in these regions.

> Fresh deployments of Cloud Volumes ONTAP in China regions are supported only in 9.12.1 GA and 9.13.0 GA. You can upgrade these versions to later patches and releases of Cloud Volumes ONTAP. If you want to deploy later Cloud Volumes ONTAP versions in China regions, contact NetApp Support.

For regional availability, refer to the Global Regions Maps for Cloud Volumes ONTAP.

05 March 2023

The following changes were introduced with the 3.9.27 release of the Connector.

Cloud Volumes ONTAP 9.13.0

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.13.0 in AWS, Azure, and Google Cloud.

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

16 TiB and 32 Tib support in Azure

Cloud Volumes ONTAP now supports 16 TiB and 32 TiB disk sizes for high-availability deployments running on managed disks in Azure.

Learn more about supported disk sizes in Azure.

MTEKM license

The Multi-tenant Encryption Key Management (MTEKM) license is now included with new and existing Cloud Volumes ONTAP systems running version 9.12.1 GA 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.

Support for environments without internet

Cloud Volumes ONTAP is now supported in any cloud environment that has complete isolation from the internet. Only node-based licensing (BYOL) is supported in these environments. Capacity-based licensing is not supported. To get started, manually install the Connector software, log in to the BlueXP console that's running on the Connector, add your BYOL license to the BlueXP digital wallet, and then deploy Cloud Volumes ONTAP.

- Install the Connector in a location without internet access
- Access the BlueXP console on the Connector
- Add an unassigned license

Flash Cache and high write speed in Google Cloud

Support for Flash Cache, high write speed, and a high maximum transmission unit (MTU) of 8,896 bytes is now available for select instances with the Cloud Volumes ONTAP 9.13.0 release.

Learn more about supported configurations by license for Google Cloud.

05 February 2023

The following changes were introduced with the 3.9.26 release of the Connector.

Placement group creation in AWS

A new configuration setting is now available for placement group creation with AWS HA single availability zone (AZ) deployments. Now you can choose to bypass failed placement group creations and allow AWS HA single AZ deployments to complete successfully.

For detailed information on how to configure the placement group creation setting, refer to Configure placement group creation for AWS HA Single AZ.

Private DNS zone configuration update

A new configuration setting is now available so that you can avoid creating a link between a private DNS zone and a virtual network when using Azure Private Links. Creation is enabled by default.

Provide BlueXP with details about your Azure Private DNS

WORM storage and data tiering

You can now enable both data tiering and WORM storage together when you create a Cloud Volumes ONTAP 9.8 system or later. Enabling data tiering with WORM storage allows you to tier the data to an object store in the cloud.

Learn about WORM storage.

1 January 2023

The following changes were introduced with the 3.9.25 release of the Connector.

Licensing packages available in Google Cloud

Optimized and Edge Cache capacity-based licensing packages are available for Cloud Volumes ONTAP in the Google Cloud Marketplace as a pay-as-you-go offering or as an annual contract.

Refer to Cloud Volumes ONTAP licensing.

Default configuration for Cloud Volumes ONTAP

The Multi-tenant Encryption Key Management (MTEKM) license is no longer included in new Cloud Volumes ONTAP deployments.

For more information on the ONTAP feature licenses automatically installed with Cloud Volumes ONTAP, refer to Default Configuration for Cloud Volumes ONTAP.

15 December 2022

Cloud Volumes ONTAP 9.12.0

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.12.0 in AWS and Google Cloud.

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

08 December 2022

Cloud Volumes ONTAP 9.12.1

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.12.1, which includes support for new features and additional cloud provider regions.

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

04 December 2022

The following changes were introduced with the 3.9.24 release of the Connector.

WORM + Cloud Backup now available during Cloud Volumes ONTAP creation

The ability to activate both write once, read many (WORM) and Cloud Backup features is now available during the Cloud Volumes ONTAP creation process.

Israel region now supported in Google Cloud

The Israel region is now supported in Google Cloud for Cloud Volumes ONTAP and the Connector for Cloud Volumes ONTAP 9.11.1 P3 and later.

15 November 2022

The following changes were introduced with the 3.9.23 release of the Connector.

ONTAP S3 license in Google Cloud

An ONTAP S3 license is now included on new and existing Cloud Volumes ONTAP systems running version 9.12.1 or later in Google Cloud Platform.

ONTAP documentation: Learn how to configure and manage S3 object storage services

06 November 2022

The following changes were introduced with the 3.9.23 release of the Connector.

Moving resource groups in Azure

You can now move a working environment from one resource group to a different resource group in Azure within the same Azure subscription.

For more information, refer to Moving resource groups.

NDMP-copy certification

NDMP-copy is now certified for use with Cloud Volume ONTAP.

For information on how to configure and use NDMP, refer to the ONTAP documentation: NDMP configuration overview.

Managed disk encryption support for Azure

A new Azure permission has been added that now allows you to encrypt all managed disks upon creation.

For more information on this new functionality, refer to Set up Cloud Volumes ONTAP to use a customer-managed key in Azure.

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.

[A screenshot of the Optimize Cost & Performance option that’s available from the Canvas after you select a Cloud Volumes ONTAP system.]

AutoSupport notifications

BlueXP 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

BlueXP 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.

[A screenshot that shows the Allow Traffic Within option that's available in the working environment wizard when selecting a security group.]

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.

[A screenshot that shows the Digital Wallet page for capacity-based licenses. The page provides an overview of the consumed capacity in your account and then breaks down the consumed capacity by licensing package.]

Elastic Volumes enhancement

BlueXP 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.

ONTAP documentation: Learn how to configure and manage S3 object storage services

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.

ONTAP documentation: Learn how to configure and manage S3 object storage services

07 June 2022

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

Cloud Volumes ONTAP 9.11.1

BlueXP 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 BlueXP so that you don't need to leave BlueXP 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 BlueXP 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 BlueXP. 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

BlueXP now limits network access when using a VNet service endpoint for connections between Cloud Volumes ONTAP and storage accounts. BlueXP 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, BlueXP 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

02 May 2022

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

Cloud Volumes ONTAP 9.11.0

BlueXP 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 BlueXP 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 release, and has now been removed.

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 Simple Storage Service (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 BlueXP creates the placement group.

Be sure to provide these permissions to each set of AWS credentials that you've added to BlueXP. 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, BlueXP will now display all existing firewall policies in a VPC.

  Previously, BlueXP 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, BlueXP 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.

[A screenshot of the service account field]

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.

09 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, BlueXP 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.

06 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.

02 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

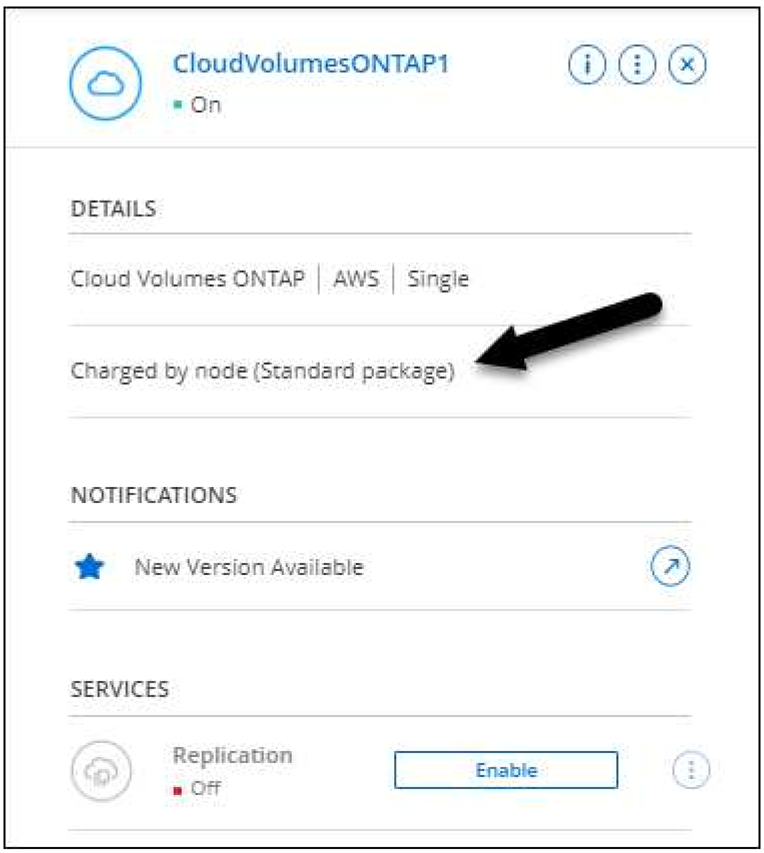
Go to the Cloud Volumes ONTAP Release Notes for more details about supported configurations.

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.

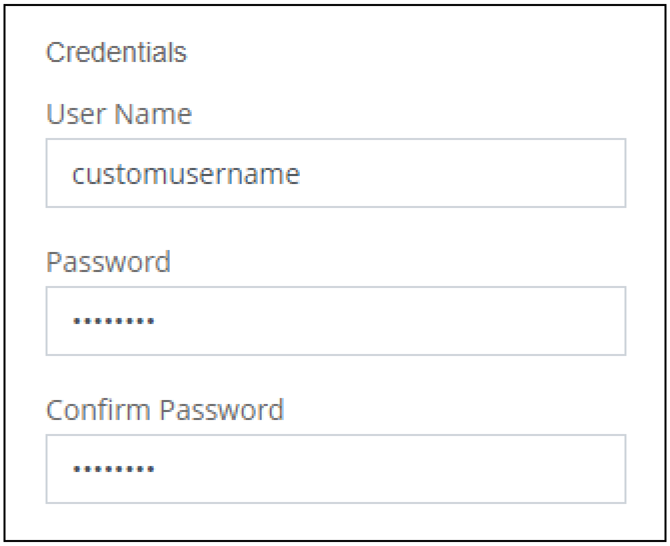
Charging method now displayed

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



Choose your user name

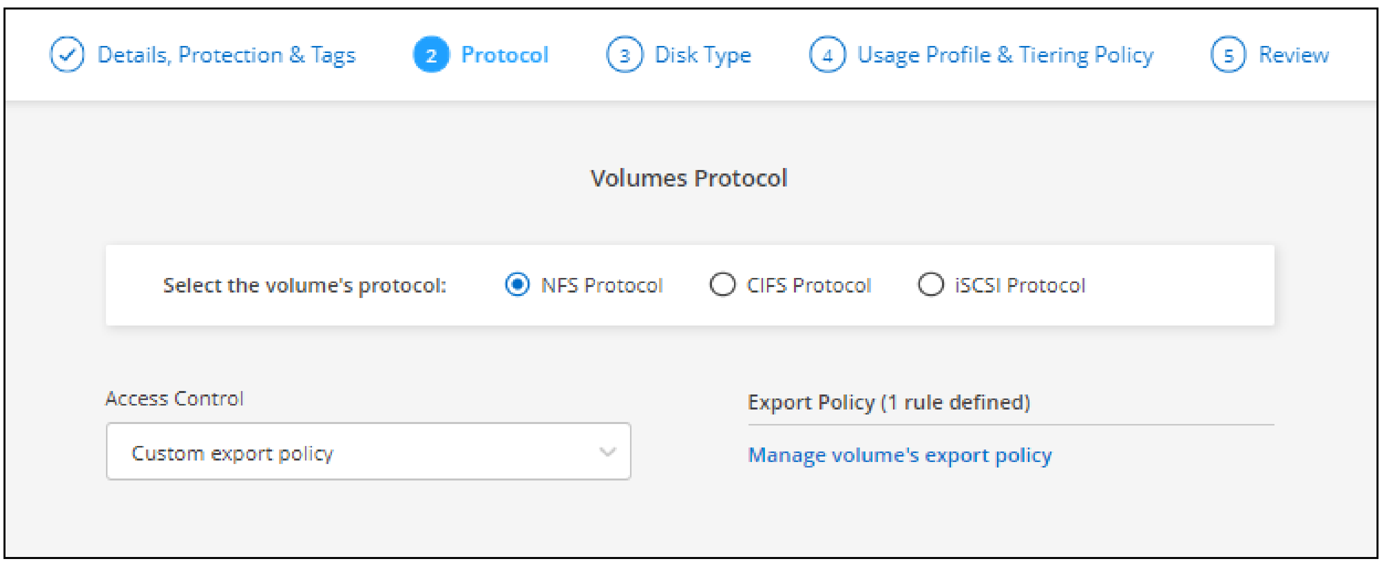
When you create a Cloud Volumes ONTAP working environment, you now have the option to enter your preferred user name, instead of the default admin user name.



Volume creation enhancements

We made a few enhancements to volume creation:

- We redesigned the create volume wizard for ease of use.
- 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

BlueXP can now deploy and manage Cloud Volumes ONTAP 9.10.1.

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

NetApp Keystone Subscriptions

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

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

- Learn more about NetApp Keystone Subscriptions.
- Learn how to get started with Keystone Subscriptions in BlueXP.

New AWS region support

Cloud Volumes ONTAP is now supported in the AWS Asia Pacific (Osaka) region (ap-northeast-3).

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.

04 October 2021

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

Cloud Volumes ONTAP 9.10.0

BlueXP 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.

02 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 BlueXP, use the API to create a Cloud Volumes ONTAP working environment that uses the key.

Learn more about these steps.

07 July 2021

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

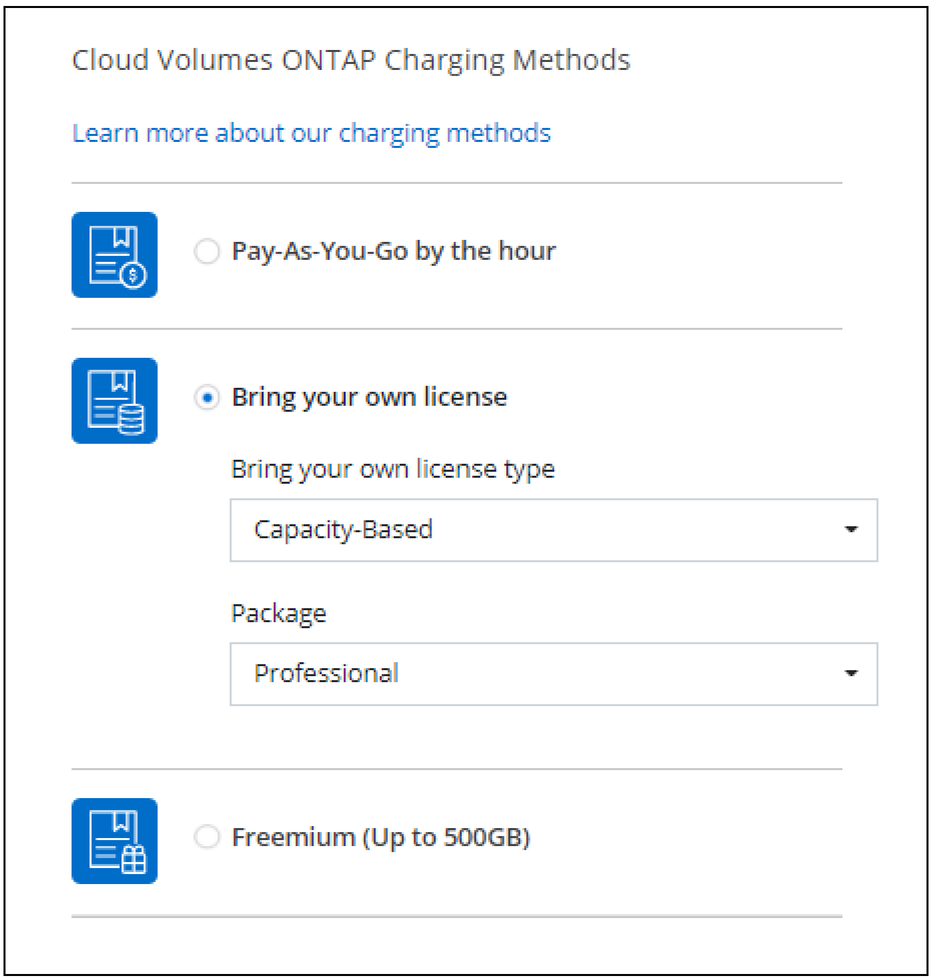
New charging methods

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.

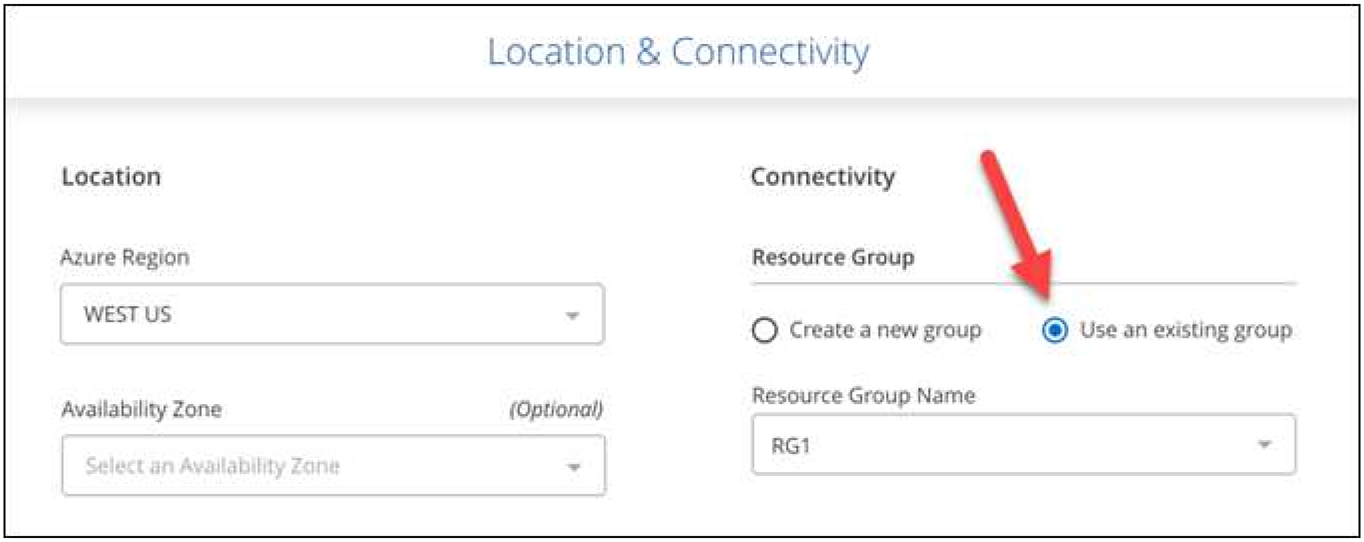
Support for m5dn.24xlarge in AWS

Starting with the 9.9.1 release, Cloud Volumes ONTAP now supports the m5dn.24xlarge instance type with the following charging methods: PAYGO Premium, bring your own license (BYOL), and Freemium.

View supported configurations for Cloud Volumes ONTAP in AWS.

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 BlueXP 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 BlueXP. View the latest Connector policy for Azure.

Blob public access now disabled in Azure

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

Azure Private Link enhancement

By default, BlueXP 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.

Balanced persistent disks in Google Cloud

Starting with the 9.9.1 release, Cloud Volumes ONTAP now supports Balanced persistent disks (pd-balanced).

These SSDs balance performance and cost by providing lower IOPS per GiB.

custom-4-16384 no longer supported in Google Cloud

The custom-4-16384 machine type is no longer supported with new Cloud Volumes ONTAP systems.

If you have an existing system running on this machine type, you can keep using it, but we recommend switching to the n2-standard-4 machine type.

View supported configurations for Cloud Volumes ONTAP in Google Cloud.

30 May 2021

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

New Professional Package in AWS

A new Professional Package enables you to bundle Cloud Volumes ONTAP and Cloud Backup Service by using an annual contract from the AWS Marketplace. Payment is per TiB. This subscription doesn't enable you to back up on-premises data.

If you choose this payment option, you can provision up to 2 PiB per Cloud Volumes ONTAP system through EBS disks and tiering to S3 object storage (single node or HA).

Go to the AWS Marketplace page to view pricing details and go to the Cloud Volumes ONTAP Release Notes to learn more about this licensing option.

Tags on EBS volumes in AWS

BlueXP now adds tags to EBS volumes when it creates a new Cloud Volumes ONTAP working environment. The tags were previously created after Cloud Volumes ONTAP was deployed.

This change can help if your organization uses service control policies (SCPs) to manage permissions.

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, BlueXP 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

BlueXP 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

BlueXP 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

BlueXP 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.

Support for gp3 disks in AWS

Cloud Volumes ONTAP now supports *General Purpose SSD (gp3)* disks, starting with the 9.7 release. gp3 disks are the lowest-cost SSDs that balance cost and performance for a broad range of workloads.

Size your system in AWS.

Cold HDD disks no longer supported in AWS

Cloud Volumes ONTAP no longer supports Cold HDD (sc1) disks.

TLS 1.2 for Azure storage accounts

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

08 Mar 2021

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

Cloud Volumes ONTAP 9.9.0

BlueXP 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 the AWS C2S environment

You can now deploy Cloud Volumes ONTAP 9.8 in the AWS Commercial Cloud Services (C2S) environment.

Deploy Cloud Volumes ONTAP in AWS Secret Cloud or AWS Top Secret Cloud.

AWS encryption with customer-managed CMKs

BlueXP has always enabled you to encrypt Cloud Volumes ONTAP data using the AWS Key Management Service (KMS). Starting with Cloud Volumes ONTAP 9.9.0, data on EBS disks and data tiered to S3 are encrypted if you select a customer-managed CMK. Previously, only EBS data would be encrypted.

Note that you'll need to provide the Cloud Volumes ONTAP IAM role with access to use the CMK.

Learn more about setting up the AWS KMS with 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).

IP address reduction in Google Cloud

We've reduced the number of IP addresses that are required for Cloud Volumes ONTAP 9.8 and later in Google Cloud. By default, one less IP address is required (we unified the intercluster LIF with the node management LIF). You also have the option to skip the creation of the SVM management LIF when using the API, which would reduce the need for an additional IP address.

Learn more about IP address requirements in Google Cloud.

Shared VPC support in Google Cloud

When you deploy a Cloud Volumes ONTAP HA pair in Google Cloud, you can now choose shared VPCs for VPC-1, VPC-2, and VPC-3. Previously, only VPC-0 could be a shared VPC. This change is supported with Cloud Volumes ONTAP 9.8 and later.

Learn more about Google Cloud networking requirements.

04 January 2021

The following changes were introduced with the 3.9.2 release of the Connector.

AWS Outposts

A few months ago, we announced that Cloud Volumes ONTAP had achieved the Amazon Web Services (AWS) Outposts Ready designation. Today, we're pleased to announce that we've validated BlueXP and Cloud Volumes ONTAP with AWS Outposts.

If you have an AWS Outpost, you can deploy Cloud Volumes ONTAP in that Outpost by selecting the Outpost VPC in the Working Environment wizard. The experience is the same as any other VPC that resides in AWS. Note that you will need to first deploy a Connector in your AWS Outpost.

There are a few limitations to point out:

- Only single node Cloud Volumes ONTAP systems are supported at this time

- The EC2 instances that you can use with Cloud Volumes ONTAP are limited to what's available in your Outpost
- Only General Purpose SSDs (gp2) are supported at this time

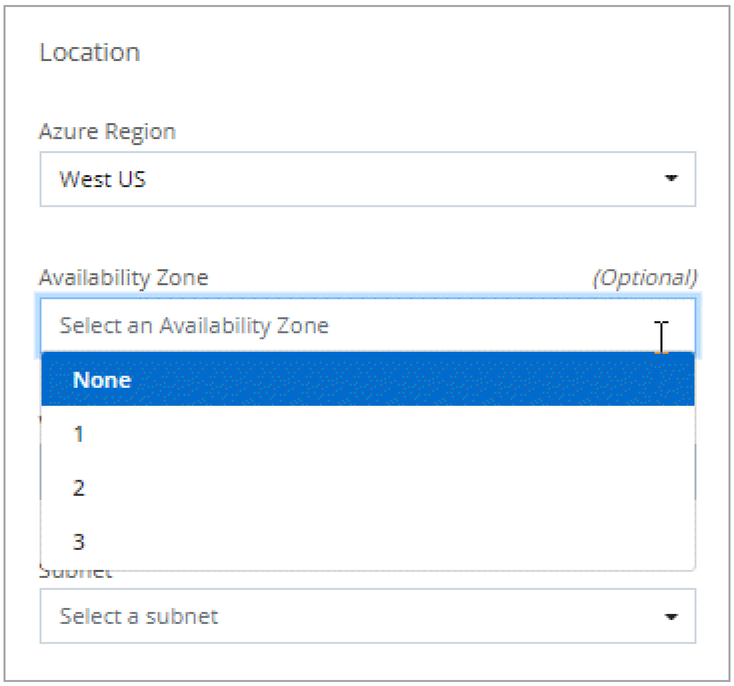
Ultra SSD VNVRAM in supported Azure regions

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, BlueXP will select one for you.



Larger disks in Google Cloud

Cloud Volumes ONTAP now supports 64 TB disks in Google Cloud.

> The maximum system capacity with disks alone remains at 256 TB due to Google Cloud limits.

New machine types in Google Cloud

Cloud Volumes ONTAP now supports the following machine types:

- n2-standard-4 with the Explore license and with BYOL
- n2-standard-8 with the Standard license and with BYOL
- n2-standard-32 with the Premium license and with BYOL

03 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, BlueXP 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 the NetApp Console. To view limitations with the Cloud Volumes ONTAP software itself, go to the Cloud Volumes ONTAP Release Notes.

Console doesn't support FlexGroup volumes creation

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

> The ability to create FlexGroup volumes in the Console is planned for a future release.

Console doesn't support S3 with Cloud Volumes ONTAP

While Cloud Volumes ONTAP supports S3 as an option for scale-out storage, the Console 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 ONTAP S3 Configuration Power Guide.

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

Console doesn't support disaster recovery for storage VMs

The Console doesn't provide any setup or orchestration support for storage VM (SVM) disaster recovery. You must use ONTAP System Manager or the ONTAP CLI.

Learn more about SVM disaster recovery.

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 NetApp Backup and Recovery to deliver backup and restore capabilities for protection, and long-term archive of your cloud data.

  Learn more about Backup and Recovery

- 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 NetApp Data Classification helps you understand data context and identify sensitive data.

  Learn more about Data Classification

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

View supported Cloud Volumes ONTAP configurations

Learn more about Cloud Volumes ONTAP

Supported ONTAP versions for Cloud Volumes ONTAP deployments

The NetApp Console enables you to choose from several different ONTAP versions when you add a Cloud Volumes ONTAP system.

Cloud Volumes ONTAP versions other than those listed here are not available for new deployments. The patch or the generic (General Availability) version in a release here represents the base version available for deployment. For details about the available patches, refer to the versioned release notes for each release.

For information on upgrade, refer to Supported upgrade paths.

AWS

Single node

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

HA pair

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1

- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Azure

Single node

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

HA pair

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Google Cloud

Single node

- 9.18.1
- 9.17.1 P1
- 9.16.1

- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA pair

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Get started in Amazon Web Services

Quick start for Cloud Volumes ONTAP in AWS

Get started with Cloud Volumes ONTAP in AWS in a few steps.

1 Create a Console agent

If you don't have a Console agent yet, you need to create one. Learn how to create a Console agent in AWS.

Note that if you want to deploy Cloud Volumes ONTAP in a subnet where no internet access is available, then you need to manually install the Console agent and access the NetApp Console user interface that's running on that Console agent. Learn how to manually install the Console agent in a location without internet access.

2 Plan your configuration

The Console 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 VPC and subnets will support connectivity between the Console agent and Cloud Volumes ONTAP.

b. Enable outbound internet access from the target VPC for NetApp AutoSupport.

   This step isn't required if you're deploying Cloud Volumes ONTAP in a location where no internet access is available.

c. Set up a VPC endpoint to the Amazon Simple Storage Service (Amazon S3) service.

   A VPC endpoint is required if you want to tier cold data from Cloud Volumes ONTAP to low-cost object storage.

Learn more about networking requirements.

4 Set up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, then you need to ensure that an active Customer Master Key (CMK) exists. You also need to modify the key policy for each CMK by adding the IAM role that provides permissions to the Console agent as a *key user*. Learn more.

5 Launch Cloud Volumes ONTAP using the Console

Click **Add System**, 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

- Create a Console agent for AWS
- Create a Console agent from the AWS Marketplace
- Install and set up a Console agent on premises
- AWS permissions for the Console agent

Plan your Cloud Volumes ONTAP configuration in AWS

When you deploy Cloud Volumes ONTAP in AWS, 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 AWS regions. View the full list of supported regions.

Newer AWS regions must be enabled before you can create and manage resources in those regions. AWS documentation: Learn how to enable a region.

Choose a supported Local Zone

Selecting a Local Zone is optional. Cloud Volumes ONTAP is supported in some AWS Local Zones including Singapore. Cloud Volumes ONTAP in AWS supports only high availability (HA) mode in a single availability zone. Single node deployments are not supported.

> Cloud Volumes ONTAP does not have support for data tiering and cloud tiering in AWS Local Zones. Additionally, Local Zones with instances that have not been qualified for Cloud Volumes ONTAP are not supported. An example of this is Miami, that is not available as a Local Zone, because it has only Gen6 instances that are unsupported and unqualified.

AWS Documentation: View the full list of Local Zones.
Local Zones must be enabled before you can create and manage resources in those zones.

AWS Documentation: Getting started with AWS Local Zones.

Choose a supported instance

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

Supported configurations for Cloud Volumes ONTAP in AWS

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 AWS

Size your system in AWS

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 an instance type, disk type, and disk size:

Instance type

- Match your workload requirements to the maximum throughput and IOPS for each EC2 instance type.
- If several users write to the system at the same time, choose an instance type that has enough CPUs to manage the requests.
- If you have an application that is mostly reads, then choose a system with enough RAM.
  - AWS Documentation: Amazon EC2 Instance Types
  - AWS Documentation: Amazon EBS-Optimized Instances

EBS disk type

At a high level, the differences between EBS disk types are as follows. To learn more about the use cases for EBS disks, refer to AWS Documentation: EBS Volume Types.

- *General Purpose SSD (gp3)* disks are the lowest-cost SSDs that balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS and throughput. gp3 disks are supported with Cloud Volumes ONTAP 9.7 and later.

  When you select a gp3 disk, the NetApp Console fills in default IOPS and throughput values that provide performance that is equivalent to a gp2 disk based on the selected disk size. You can increase the values to get better performance at a higher cost, but we do not support lower values because it can result in inferior performance. In short, stick with the default values or increase them. Don't lower them. AWS Documentation: Learn more about gp3 disks and their performance.

  Note that Cloud Volumes ONTAP supports the Amazon EBS Elastic Volumes feature with gp3 disks. Learn more about Elastic Volumes support.

- *General Purpose SSD (gp2)* disks balance cost and performance for a broad range of workloads. Performance is defined in terms of IOPS.
- *Provisioned IOPS SSD (io1)* disks are for critical applications that require the highest performance at a higher cost.

  Note that Cloud Volumes ONTAP supports the Amazon EBS Elastic Volumes feature with io1 disks. Learn more about Elastic Volumes support.

- *Throughput Optimized HDD (st1)* disks are for frequently accessed workloads that require fast and consistent throughput at a lower price.

  > Data tiering to Amazon Simple Storage Service (Amazon S3) is not supported if your Cloud Volumes ONTAP system is in an AWS Local Zone, because accessing the Amazon S3 buckets outside of the Local Zone involves higher latency and impacts Cloud Volumes ONTAP activities.

EBS disk size

If you choose a configuration that doesn't support the Amazon EBS Elastic Volumes feature, then you need to choose an initial disk size when you launch a Cloud Volumes ONTAP system. After that, you can let the Console manage a system's capacity for you, but if you want to create aggregates yourself, be aware of the following:

- All disks in an aggregate must be the same size.
- The performance of EBS disks is tied to disk size. The size determines the baseline IOPS and maximum burst duration for SSD disks and the baseline and burst throughput for HDD disks.
- Ultimately, you should choose the disk size that gives you the *sustained performance* that you need.
- Even if you do choose larger disks (for example, six 4 TiB disks), you might not get all of the IOPS because the EC2 instance can reach its bandwidth limit.

  For more details about EBS disk performance, refer to AWS Documentation: EBS Volume Types.

  As noted above, choosing a disk size is not supported with Cloud Volumes ONTAP configurations that support the Amazon EBS Elastic Volumes feature. Learn more about Elastic Volumes support.

View default system disks

In addition to the storage for user data, the Console 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 AWS.

The Console agent also requires a system disk. View details about the Console agent's default configuration.

Prepare to deploy Cloud Volumes ONTAP in an AWS Outpost

If you have an AWS Outpost, you can deploy Cloud Volumes ONTAP in that Outpost by selecting the Outpost VPC during the deployment process. The experience is the same as any other VPC that resides in AWS. Note that you will need to first deploy a Console agent in your AWS Outpost.

There are a few limitations to point out:

- Only single node Cloud Volumes ONTAP systems are supported at this time
- The EC2 instances that you can use with Cloud Volumes ONTAP are limited to what's available in your Outpost
- Only General Purpose SSDs (gp2) are supported at this time

Collect networking information

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

Single node or HA pair in a single AZ

AWS information	Your value
Region	
VPC	
Subnet	

AWS information	Your value
Security group (if using your own)	

HA pair in multiple AZs

AWS information	Your value
Region	
VPC	
Security group (if using your own)	
Node 1 availability zone	
Node 1 subnet	
Node 2 availability zone	
Node 2 subnet	
Mediator availability zone	
Mediator subnet	
Key pair for the mediator	
Floating IP address for cluster management port	
Floating IP address for data on node 1	
Floating IP address for data on node 2	
Route tables for floating IP addresses	

Choose a write speed

The Console 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 the Console, 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.

Set up your networking

Set up AWS networking for Cloud Volumes ONTAP

The NetApp Console handles the set up of networking components for Cloud Volumes ONTAP, such as IP addresses, netmasks, and routes. You need to make sure that outbound internet access is available, that enough private IP addresses are available, that the right connections are in place, and more.

General requirements

Ensure that you have fulfilled the following requirements in AWS.

Outbound internet access for Cloud Volumes ONTAP nodes

Cloud Volumes ONTAP systems require outbound internet access for accessing external endpoints for various functions. Cloud Volumes ONTAP can’t operate properly if these endpoints are blocked in environments with strict security requirements.

The Console agent contacts several endpoints for day-to-day operations. For information about the endpoints used, refer to View endpoints contacted from the Console agent and Prepare networking for using the Console.

Cloud Volumes ONTAP endpoints

Cloud Volumes ONTAP uses these endpoints to communicate with various services.

Endpoints	Applicable for	Purpose	Deployment modes	Impact if endpoint is not available
https://netapp-cloud-account.auth0.com	Authentication	Used for authentication in the Console.	Standard and restricted modes.	User authentication fails and the following services remain unavailable: • Cloud Volumes ONTAP services • ONTAP services • Protocols and proxy services

Endpoints	Applicable for	Purpose	Deployment modes	Impact if endpoint is not available
https://api.bluexp.netapp.com/tenancy	Tenancy	Used to retrieve Cloud Volumes ONTAP resource from the Console to authorize resources and users.	Standard and restricted modes.	Cloud Volumes ONTAP resources and the users are not authorized.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Used to send AutoSupport telemetry data to NetApp support.	Standard and restricted modes.	AutoSupport information remains undelivered.
The exact commercial endpoint for AWS service (suffixed with `amazonaws.com`) depends on the AWS region that you are using. Refer to the AWS documentation for details.	• CloudFormation • Elastic Compute Cloud (EC2) • Identity and Access Management (IAM) • Key Management Service (KMS) • Security Token Service (STS) • Amazon Simple Storage Service (S3)	Communication with AWS services.	Standard and private modes.	Cloud Volumes ONTAP cannot communicate with AWS service to perform specific operations in AWS.
The exact government endpoint for AWS service depends on the AWS region that you are using. The endpoints are suffixed with `amazonaws.com` and `c2s.ic.gov`. Refer to AWS SDK and AWS Documentation for more information.	• CloudFormation • Elastic Compute Cloud (EC2) • Identity and Access Management (IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Communication with AWS services.	Restricted mode.	Cloud Volumes ONTAP cannot communicate with AWS service to perform specific operations in AWS.

Outbound internet access for the HA mediator

The HA mediator instance must have an outbound connection to the AWS EC2 service so it can assist with storage failover. To provide the connection, you can add a public IP address, specify a proxy server, or use a manual option.

The manual option can be a NAT gateway or an interface VPC endpoint from the target subnet to the AWS

EC2 service. For details about VPC endpoints, refer to the AWS Documentation: Interface VPC Endpoints (AWS PrivateLink).

Network proxy configuration of NetApp Console agent

You can use the proxy servers configuration of the NetApp Console agent to enable outbound internet access from Cloud Volumes ONTAP. The Console supports two types of proxies:

- **Explicit proxy**: The outbound traffic from Cloud Volumes ONTAP uses the HTTP address of the proxy server specified during the proxy configuration of the Console agent. The administrator might also have configured user credentials and root CA certificates for additional authentication. If a root CA certificate is available for the explicit proxy, make sure to obtain and upload the same certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.
- **Transparent proxy**: The network is configured to automatically route outbound traffic from Cloud Volumes ONTAP through the proxy for the Console agent. When setting up a transparent proxy, the administrator needs to provide only a root CA certificate for connectivity from Cloud Volumes ONTAP, not the HTTP address of the proxy server. Make sure that you obtain and upload the same root CA certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.

For information about configuring proxy servers, refer to the Configure the Console agent to use a proxy server.

Private IP addresses

The Console automatically allocates the required number of private IP addresses to Cloud Volumes ONTAP. You need to ensure that your networking has enough private IP addresses available.

The number of LIFs that the Console allocates for Cloud Volumes ONTAP depends on whether you deploy a single-node system or an HA pair. A LIF is an IP address associated with a physical port.

IP addresses for a single-node system

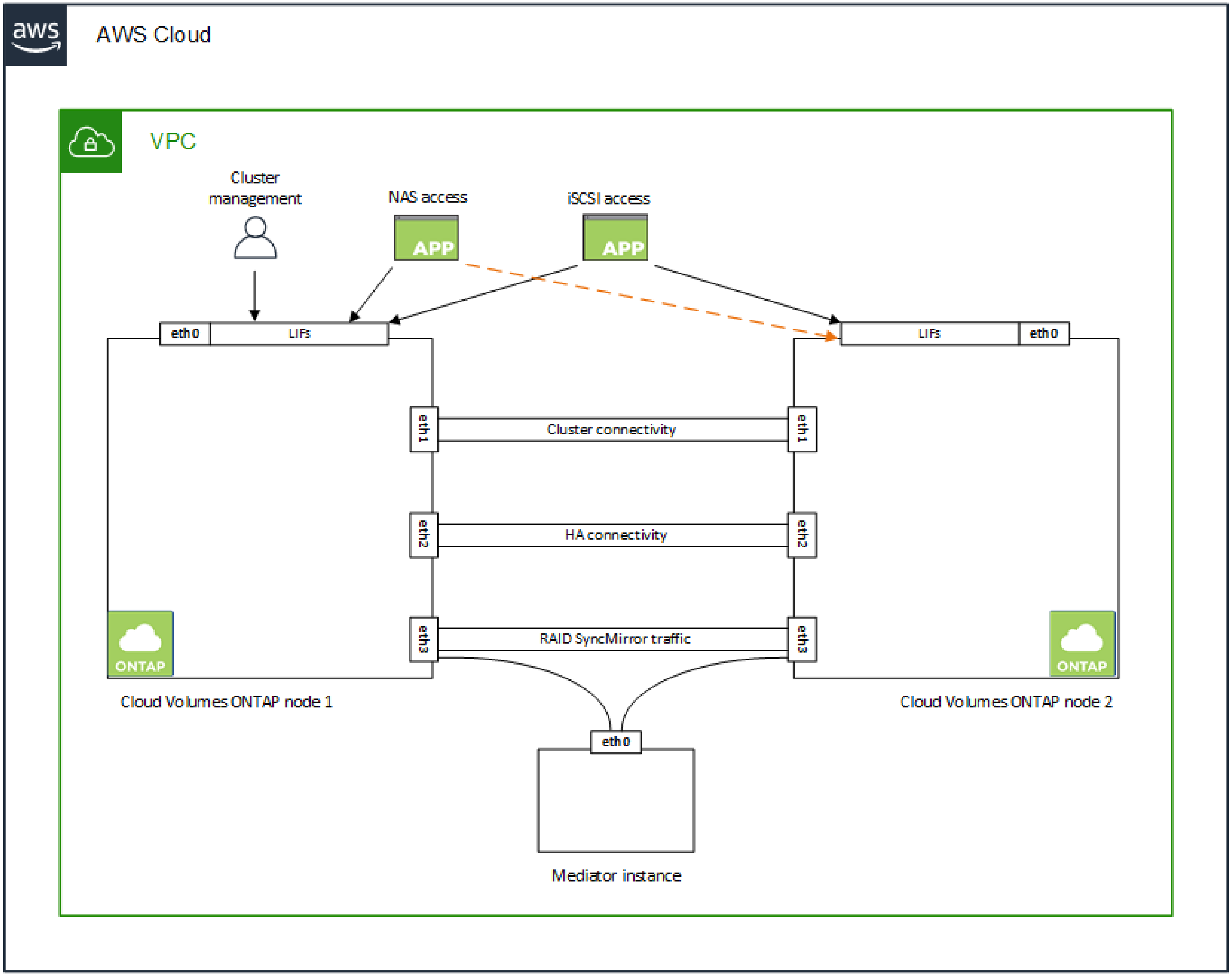
The Console allocates 6 IP addresses to a single-node system.

The following table provides details about the LIFs that are associated with each private IP address.

LIF	Purpose
Cluster management	Administrative management of the entire cluster (HA pair).
Node management	Administrative management of a node.
Intercluster	Cross-cluster communication, backup, and replication.
NAS data	Client access over NAS protocols.
iSCSI data	Client access over the iSCSI protocol. Also used by the system for other important networking workflows. This LIF is required and should not be deleted.
Storage VM management	A storage VM management LIF is used with management tools like SnapCenter.

IP addresses for HA pairs

HA pairs require more IP addresses than a single-node system does. These IP addresses are spread across different ethernet interfaces, as shown in the following image:



The number of private IP addresses required for an HA pair depends on which deployment model you choose. An HA pair deployed in a *single* AWS Availability Zone (AZ) requires 15 private IP addresses, while an HA pair deployed in *multiple* AZs requires 13 private IP addresses.

The following tables provide details about the LIFs that are associated with each private IP address.

Table 1. LIFs for HA pairs in a single AZ

LIF	Interface	Node	Purpose
Cluster management	eth0	node 1	Administrative management of the entire cluster (HA pair).
Node management	eth0	node 1 and node 2	Administrative management of a node.
Intercluster	eth0	node 1 and node 2	Cross-cluster communication, backup, and replication.
NAS data	eth0	node 1	Client access over NAS protocols.

LIF	Interface	Node	Purpose
iSCSI data	eth0	node 1 and node 2	Client access over the iSCSI protocol. Also used by the system for other important networking workflows. These LIFs are required and should not be deleted.
Cluster connectivity	eth1	node 1 and node 2	Enables the nodes to communicate with each other and to move data within the cluster.
HA connectivity	eth2	node 1 and node 2	Communication between the two nodes in case of failover.
RSM iSCSI traffic	eth3	node 1 and node 2	RAID SyncMirror iSCSI traffic, as well as communication between the two Cloud Volumes ONTAP nodes and the mediator.
Mediator	eth0	Mediator	A communication channel between the nodes and the mediator to assist in storage takeover and giveback processes.

Table 2. LIFs for HA pairs in multiple AZs

LIF	Interface	Node	Purpose
Node management	eth0	node 1 and node 2	Administrative management of a node.
Intercluster	eth0	node 1 and node 2	Cross-cluster communication, backup, and replication.
iSCSI data	eth0	node 1 and node 2	Client access over the iSCSI protocol. These LIFs also manage the migration of floating IP addresses between nodes. These LIFs are required and should not be deleted.
Cluster connectivity	eth1	node 1 and node 2	Enables the nodes to communicate with each other and to move data within the cluster.
HA connectivity	eth2	node 1 and node 2	Communication between the two nodes in case of failover.
RSM iSCSI traffic	eth3	node 1 and node 2	RAID SyncMirror iSCSI traffic, as well as communication between the two Cloud Volumes ONTAP nodes and the mediator.
Mediator	eth0	Mediator	A communication channel between the nodes and the mediator to assist in storage takeover and giveback processes.

When deployed in multiple Availability Zones, several LIFs are associated with floating IP addresses, which don't count against the AWS private IP limit.

Security groups

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

> Looking for information about the Console agent? View security group rules for the Console agent

Connection for data tiering

If you want to use EBS as a performance tier and Amazon S3 as a capacity tier, you must ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, refer to the AWS Documentation: Creating a Gateway Endpoint.

When you create the VPC Endpoint, be sure to select the region, VPC, and route table that corresponds to the Cloud Volumes ONTAP instance. You must also modify the security group to add an outbound HTTPS rule that enables traffic to the S3 endpoint. Otherwise, Cloud Volumes ONTAP cannot connect to the S3 service.

If you experience any issues, refer to the AWS Support Knowledge Center: Why can't I connect to an S3 bucket using a gateway VPC endpoint?

Connections to ONTAP systems

To replicate data between a Cloud Volumes ONTAP system in AWS and ONTAP systems in other networks, you must have a VPN connection between the AWS VPC and the other network—for example, your corporate network. For instructions, refer to the AWS Documentation: Setting Up an AWS VPN Connection.

DNS and Active Directory for CIFS

If you want to provision CIFS storage, you must set up DNS and Active Directory in AWS or extend your on-premises setup to AWS.

The DNS server must provide name resolution services for the Active Directory environment. You can configure DHCP option sets to use the default EC2 DNS server, which must not be the DNS server used by the Active Directory environment.

For instructions, refer to the AWS Documentation: Active Directory Domain Services on the AWS Cloud: Quick Start Reference Deployment.

VPC sharing

Starting with the 9.11.1 release, Cloud Volumes ONTAP HA pairs are supported in AWS with VPC sharing. VPC sharing enables your organization to share subnets with other AWS accounts. To use this configuration, you must set up your AWS environment and then deploy the HA pair using the API.

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

Requirements for HA pairs in multiple AZs

Additional AWS networking requirements apply to Cloud Volumes ONTAP HA configurations that use multiple Availability Zones (AZs). You should review these requirements before you launch an HA pair because you must enter the networking details in the Console when you add a Cloud Volumes ONTAP system.

To understand how HA pairs work, refer to High-availability pairs.

Availability Zones

This HA deployment model uses multiple AZs to ensure high availability of your data. You should use a dedicated AZ for each Cloud Volumes ONTAP instance and the mediator instance, which provides a communication channel between the HA pair.

A subnet should be available in each Availability Zone.

Floating IP addresses for NAS data and cluster/SVM management

HA configurations in multiple AZs use floating IP addresses that migrate between nodes if failures occur. They are not natively accessible from outside the VPC, unless you set up an AWS transit gateway.

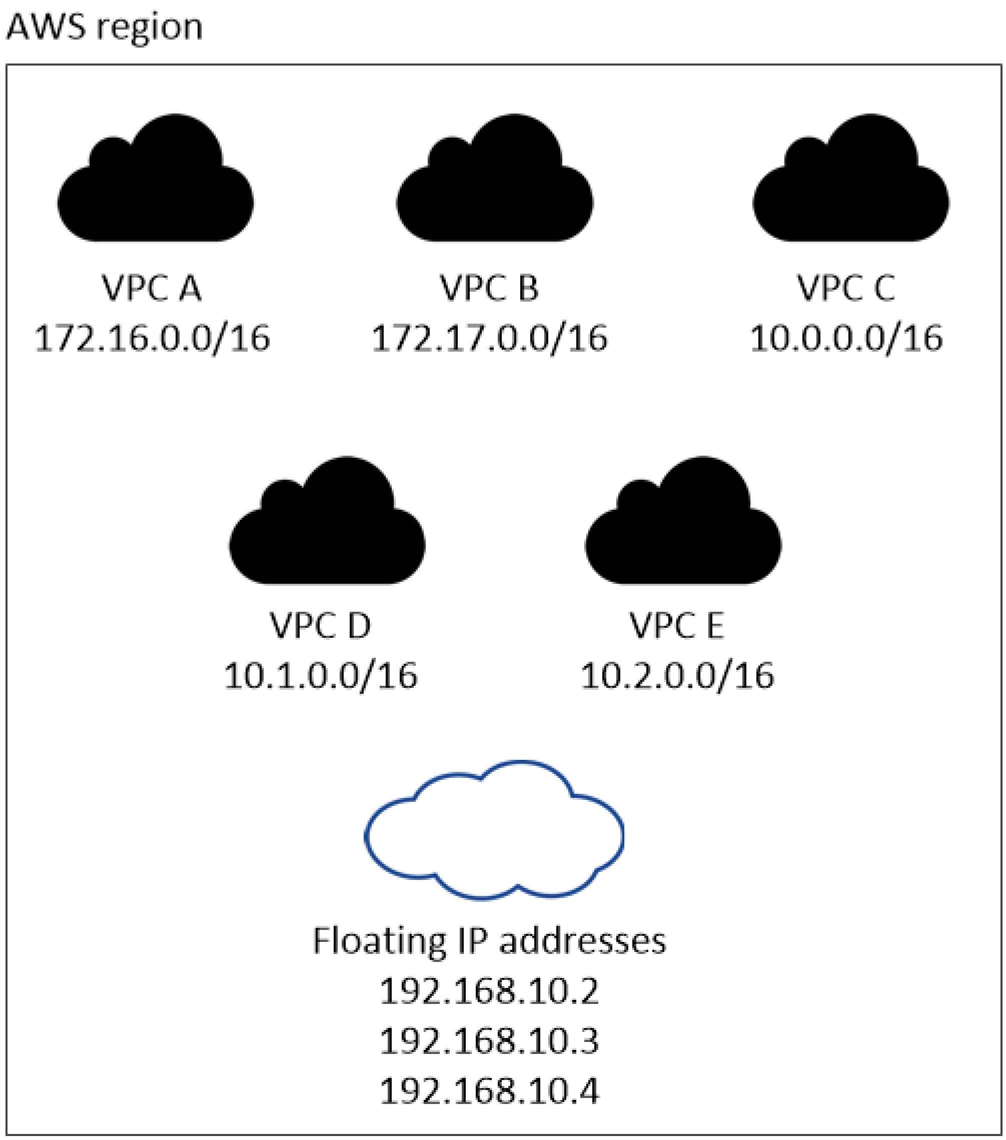
One floating IP address is for cluster management, one is for NFS/CIFS data on node 1, and one is for NFS/CIFS data on node 2. A fourth floating IP address for SVM management is optional.

> A floating IP address is required for the SVM management LIF if you use SnapDrive for Windows or SnapCenter with the HA pair.

You need to enter the floating IP addresses when you add a Cloud Volumes ONTAP HA system. The Console allocates the IP addresses to the HA pair when it launches the system.

The floating IP addresses must be outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. Think of the floating IP addresses as a logical subnet that's outside of the VPCs in your region.

The following example shows the relationship between floating IP addresses and the VPCs in an AWS region. While the floating IP addresses are outside the CIDR blocks for all VPCs, they're routable to subnets through route tables.



> The Console automatically creates static IP addresses for iSCSI access and for NAS access from clients outside the VPC. You don't need to meet any requirements for these types of IP addresses.

Transit gateway to enable floating IP access from outside the VPC

If needed, set up an AWS transit gateway to enable access to an HA pair's floating IP addresses from outside the VPC where the HA pair resides.

Route tables

After you specify the floating IP addresses, you are then prompted to select the route tables that should include routes to the floating IP addresses. This enables client access to the HA pair.

If you have just one route table for the subnets in your VPC (the main route table), then the Console automatically adds the floating IP addresses to that route table. If you have more than one route table, it's very important to select the correct route tables when launching the HA pair. Otherwise, some clients might not have access to Cloud Volumes ONTAP.

For example, you might have two subnets that are associated with different route tables. If you select route table A, but not route table B, then clients in the subnet associated with route table A can access the HA pair, but clients in the subnet associated with route table B can’t.

For more information about route tables, refer to the AWS Documentation: Route Tables.

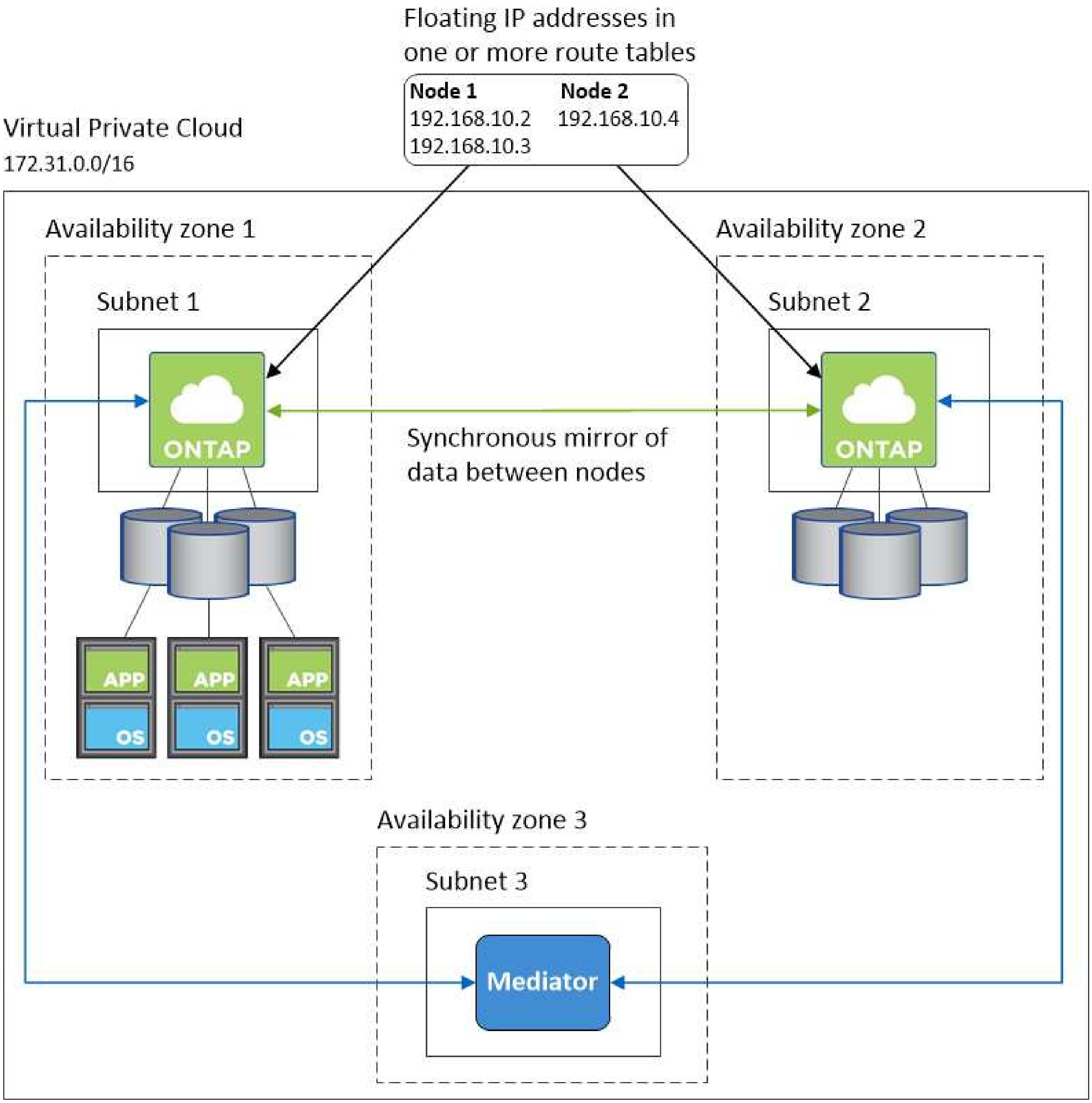
Connection to NetApp management tools

To use NetApp management tools with HA configurations that are in multiple AZs, you have two connection options:

1. Deploy the NetApp management tools in a different VPC and set up an AWS transit gateway. The gateway enables access to the floating IP address for the cluster management interface from outside the VPC.
2. Deploy the NetApp management tools in the same VPC with a similar routing configuration as NAS clients.

Example HA configuration

The following image illustrates the networking components specific to an HA pair in multiple AZs: three Availability Zones, three subnets, floating IP addresses, and a route table.



Requirements for the Console agent

If you haven't created a Console agent yet, you should review networking requirements.

- View networking requirements for the Console agent
- Security group rules in AWS

Related topics

- Verify AutoSupport setup for Cloud Volumes ONTAP
- Learn about ONTAP internal ports.

Set up an AWS transit gateway for Cloud Volumes ONTAP HA pairs

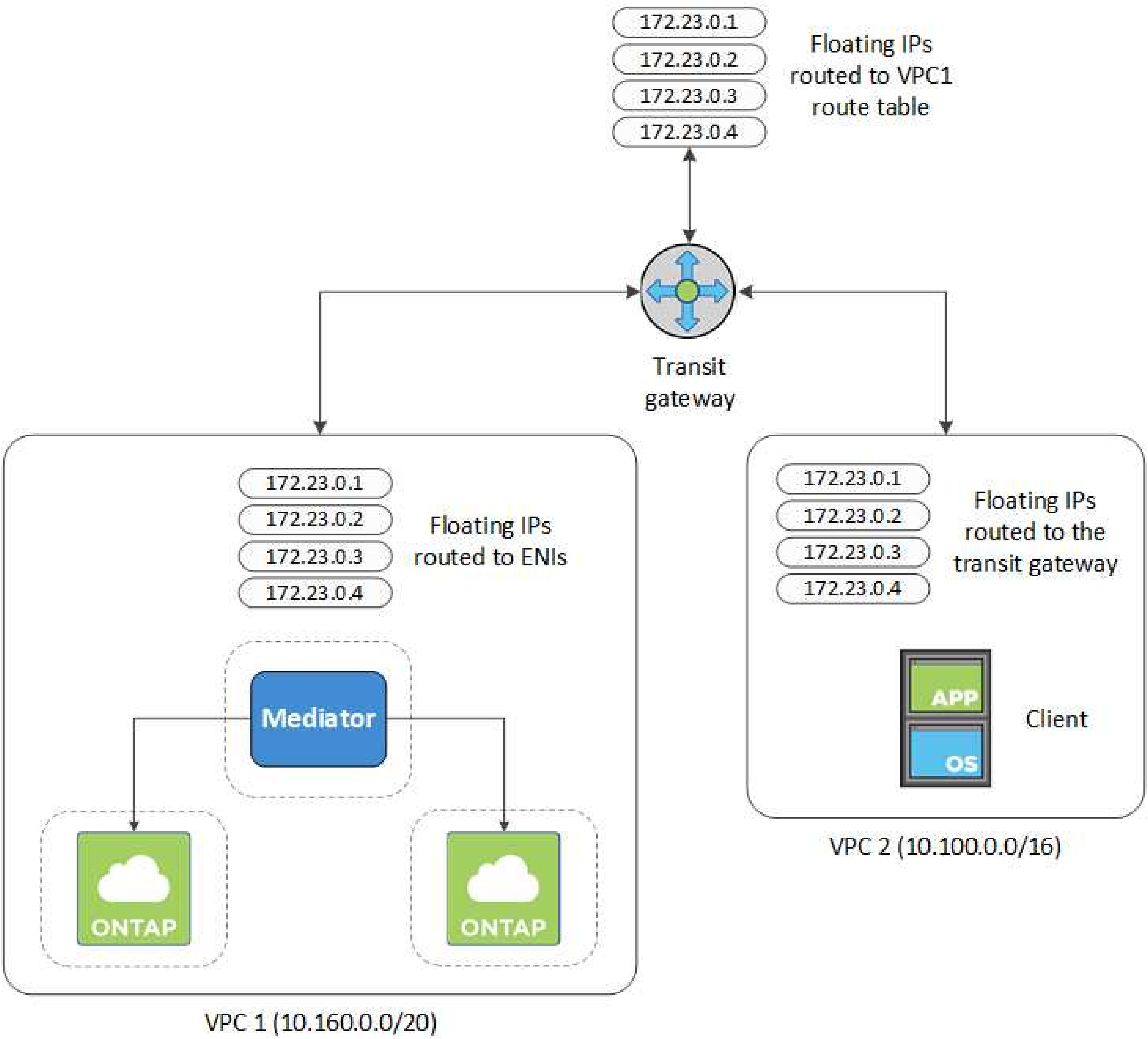
Set up an AWS transit gateway to enable access to an HA pair's floating IP addresses from outside the VPC where the HA pair resides.

When a Cloud Volumes ONTAP HA configuration is spread across multiple AWS Availability Zones, floating IP addresses are required for NAS data access from within the VPC. These floating IP addresses can migrate between nodes when failures occur, but they are not natively accessible from outside the VPC. Separate private IP addresses provide data access from outside the VPC, but they don't provide automatic failover.

Floating IP addresses are also required for the cluster management interface and the optional SVM management LIF.

If you set up an AWS transit gateway, you enable access to the floating IP addresses from outside the VPC where the HA pair resides. That means NAS clients and NetApp management tools outside the VPC can access the floating IPs.

Here's an example that shows two VPCs connected by a transit gateway. An HA system resides in one VPC, while a client resides in the other. You could then mount a NAS volume on the client using the floating IP address.

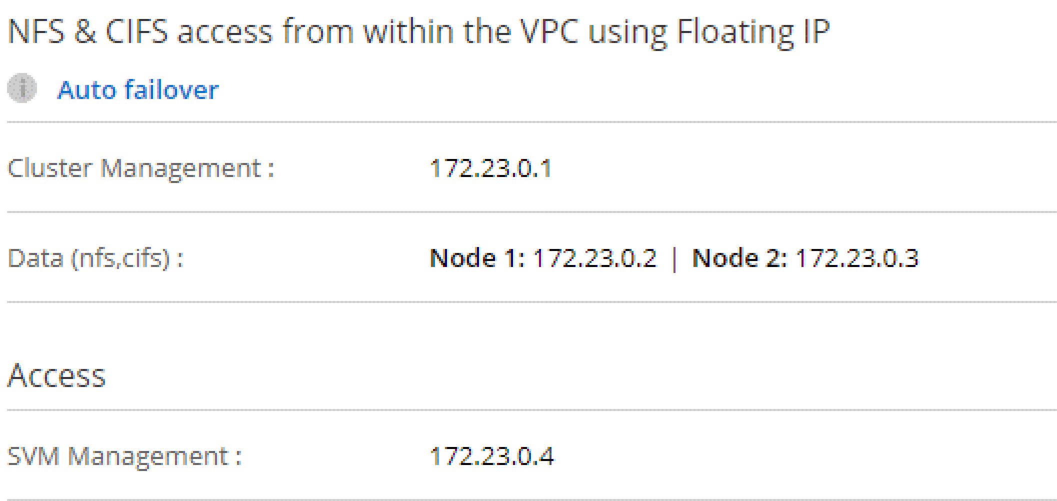


The following steps illustrate how to set up a similar configuration.

Steps

1. Create a transit gateway and attach the VPCs to the gateway.
2. Associate the VPCs with the transit gateway route table.
   a. In the **VPC** service, click **Transit Gateway Route Tables**.
   b. Select the route table.
   c. Click **Associations** and then select **Create association**.
   d. Choose the attachments (the VPCs) to associate and then click **Create association**.
3. Create routes in the transit gateway's route table by specifying the HA pair's floating IP addresses.

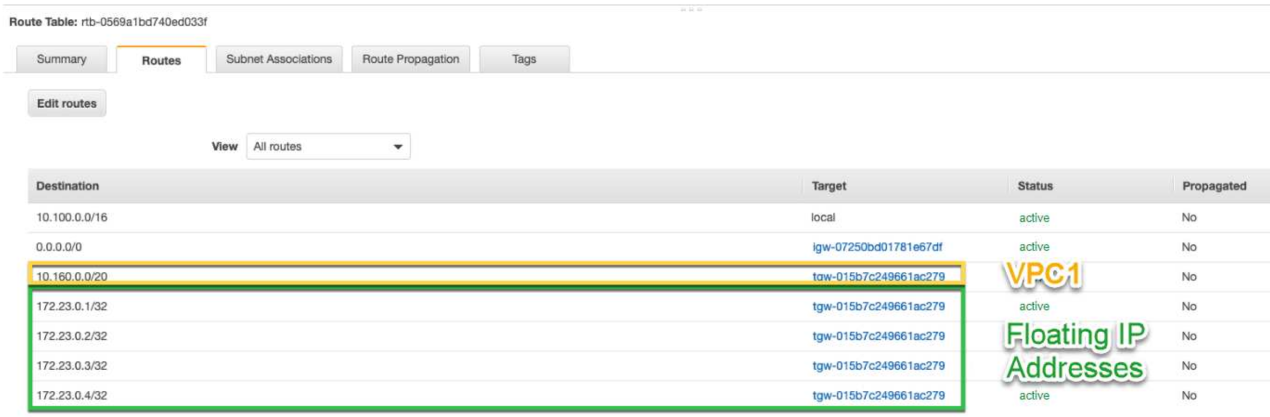
   You can find the floating IP addresses on the system information page in the NetApp Console. Here's an example:



The following sample image shows the route table for the transit gateway. It includes routes to the CIDR blocks of the two VPCs and four floating IP addresses used by Cloud Volumes ONTAP.

4. Modify the route table of VPCs that need to access the floating IP addresses.
    a. Add route entries to the floating IP addresses.
    b. Add a route entry to the CIDR block of the VPC where the HA pair resides.

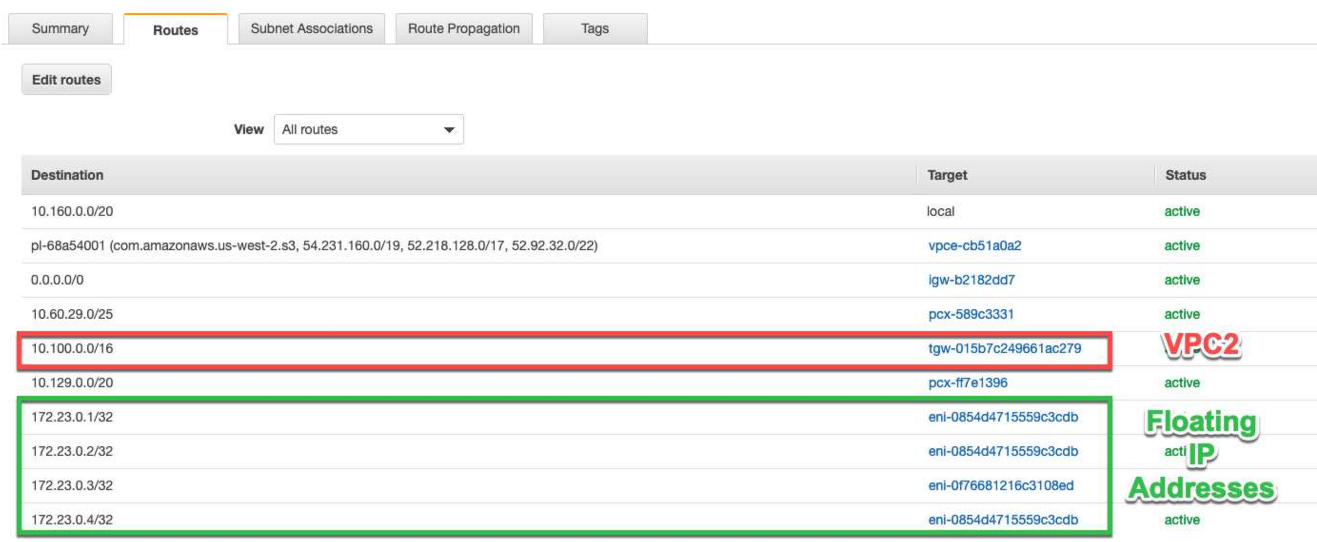
       The following sample image shows the route table for VPC 2, which includes routes to VPC 1 and the floating IP addresses.



5. Modify the route table for the HA pair's VPC by adding a route to the VPC that needs access to the floating IP addresses.

   This step is important because it completes the routing between the VPCs.

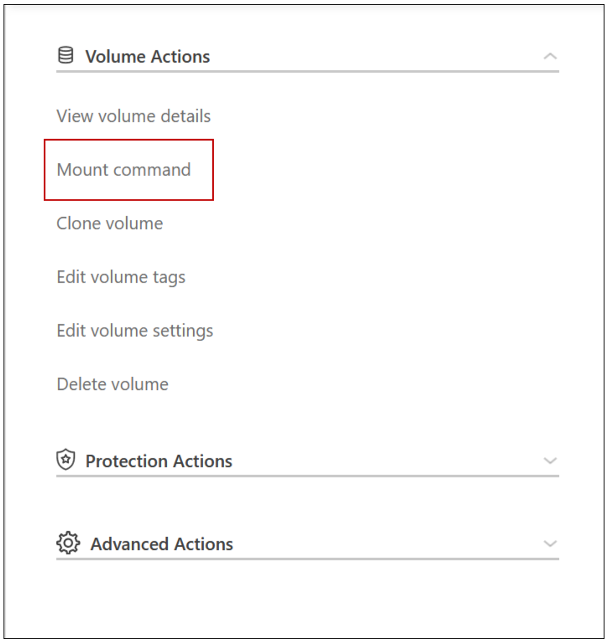
   The following sample image shows the route table for VPC 1. It includes a route to the floating IP addresses and to VPC 2, which is where a client resides. The Console automatically added the floating IPs to the route table when it deployed the HA pair.



6. Update the security groups settings to All traffic for the VPC.
   a. Under Virtual Private Cloud, click **Subnets**.
   b. Click the **Route table** tab, select the desired environment for one of the floating IP addresses for an HA pair.
   c. Click **Security groups**.
   d. Select **Edit Inbound Rules**.
   e. Click **Add rule**.
   f. Under Type, select **All traffic**, and then select the VPC IP address.
   g. Click **Save Rules** to apply the changes.
7. Mount volumes to clients using the floating IP address.

   You can find the correct IP address in the Console through the **Mount Command** option under the Manage

Volumes panel in the Console.



8. If you’re mounting an NFS volume, configure the export policy to match the subnet of the client VPC.

   Learn how to edit a volume.

Related links

- High-availability pairs in AWS
- Networking requirements for Cloud Volumes ONTAP in AWS

Deploy Cloud Volumes ONTAP HA pairs in an AWS shared subnet

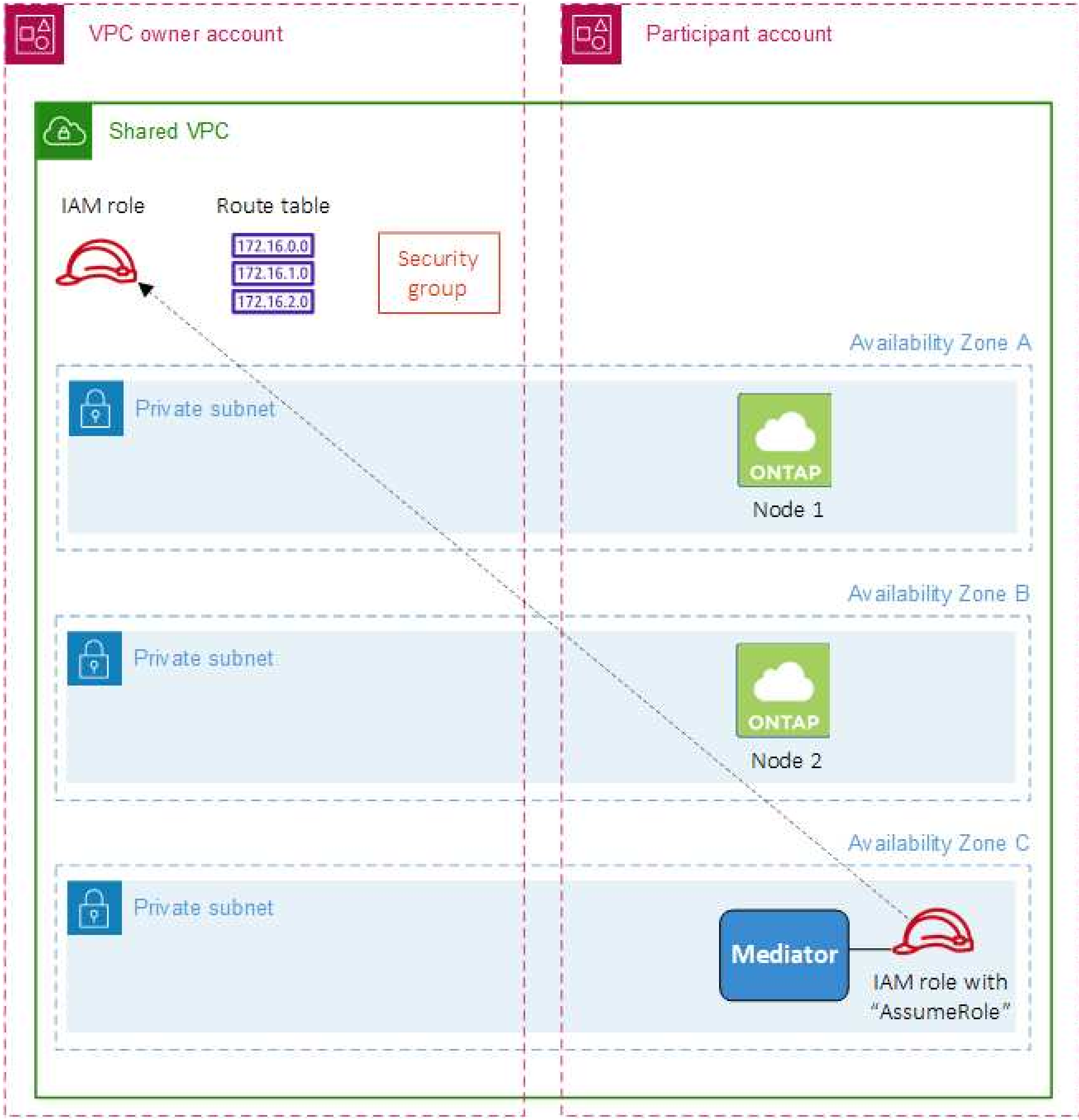
Starting with the 9.11.1 release, Cloud Volumes ONTAP HA pairs are supported in AWS with VPC sharing. VPC sharing enables your organization to share subnets with other AWS accounts. To use this configuration, you must set up your AWS environment and then deploy the HA pair using the API.

With VPC sharing, a Cloud Volumes ONTAP HA configuration is spread across two accounts:

- The VPC owner account, which owns the networking (the VPC, subnets, route tables, and Cloud Volumes ONTAP security group)
- The participant account, where the EC2 instances are deployed in shared subnets (this includes the two HA nodes and the mediator)

In the case of a Cloud Volumes ONTAP HA configuration that is deployed across multiple Availability Zones, the HA mediator needs specific permissions to write to the route tables in the VPC owner account. You need to provide those permissions by setting up an IAM role that the mediator can assume.

The following image shows the components involved this deployment:



As described in the steps below, you'll need to share the subnets with the participant account, and then create the IAM role and security group in the VPC owner account.

When you create the Cloud Volumes ONTAP system, the NetApp Console automatically creates and attaches an IAM role to the mediator. This role assumes the IAM role that you created in the VPC owner account in order to make changes to the route tables associated with the HA pair.

Steps

1. Share the subnets in the VPC owner account with the participant account.

   This step is required to deploy the HA pair in shared subnets.

   AWS documentation: Share a subnet

2. In the VPC owner account, create a security group for Cloud Volumes ONTAP.

   Refer to the security group rules for Cloud Volumes ONTAP. Note that you don't need to create a security group for the HA mediator. The Console does that for you.

3. In the VPC owner account, create an IAM role that includes the following permissions:

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. Use the API to create a new Cloud Volumes ONTAP system.

   Note that you must specify the following fields:

   - "securityGroupId"

     The "securityGroupId" field should specify the security group that you created in the VPC owner account (see step 2 above).

   - "assumeRoleArn" in the "haParams" object

     The "assumeRoleArn" field should include the ARN of the IAM role that you created in the VPC owner account (see step 3 above).

     For example:

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

     Learn about the Cloud Volumes ONTAP API

Configure placement group creation for Cloud Volumes ONTAP HA pairs in AWS single AZs

Cloud Volumes ONTAP high-availability (HA) deployments in AWS single availability Zone (AZ) can fail and roll back if the creation of the placement group fails. Creation of the placement group also fails and the deployment rolls back if the Cloud Volumes ONTAP node and mediator instance are not available. To avoid this, you can modify the configuration to allow the deployment to finish even if the placement group creation fails.

On bypassing the rollback process, the Cloud Volumes ONTAP deployment process completes successfully, and notifies you that the placement group creation is incomplete.

Steps

1. Use SSH to connect to the NetApp Console agent host and log in.
2. Navigate to `/opt/application/netapp/cloudmanager/docker_occm/data`.
3. Edit `app.conf` by changing the value of the `rollback-on-placement-group-failure` parameter to `false`. The default value of this parameter is `true`.

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. Save the file and log off the Console agent. You don’t need to restart the Console agent.

AWS security group inbound and outbound rules for Cloud Volumes ONTAP

The NetApp Console creates AWS 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 to use your own security groups.

Rules for Cloud Volumes ONTAP

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

Inbound rules

When you add a Cloud Volumes ONTAP system and choose a predefined security group, you can choose to allow traffic within one of the following:

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

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the ONTAP System Manager web console using the IP address of the cluster management LIF
HTTPS	443	Connectivity with the Console agent and HTTPS access to the ONTAP System Manager web console using the IP address of the cluster management LIF

Protocol	Port	Purpose
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
UDP	635	NFS mount
UDP	2049	NFS server daemon
UDP	4045	NFS lock daemon
UDP	4046	Network status monitor for NFS
UDP	4049	NFS rquotad protocol

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.

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

Service	Protocol	Port	Source	Destination	Purpose
AutoSupport	HTTPS	443	Node management LIF	mysupport.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	mysupport.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Console agent	Sending AutoSupport messages through a proxy server on the Console agent, if an outbound internet connection isn't available
Backup to S3	TCP	5010	Intercluster LIF	Backup endpoint or restore endpoint	Back up and restore operations for the Backup to S3 feature
Cluster	All traffic	All traffic	All LIFs on one node	All LIFs on the other node	Intercluster communications (Cloud Volumes ONTAP HA only)
	TCP	3000	Node management LIF	HA mediator	ZAPI calls (Cloud Volumes ONTAP HA only)
	ICMP	1	Node management LIF	HA mediator	Keep alive (Cloud Volumes ONTAP HA only)
Configuration backups	HTTP	80	Node management LIF	http://<console-agent-IP-address>/occm/offboxconfig	Send configuration backups to the Console agent. ONTAP documentation
DHCP	UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
DHCPS	UDP	67	Node management LIF	DHCP	DHCP server
DNS	UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Node management LIF	Destination servers	NDMP copy
SMTP	TCP	25	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	TCP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	161	Node management LIF	Monitor server	Monitoring by SNMP traps
	TCP	162	Node management LIF	Monitor server	Monitoring by SNMP traps
	UDP	162	Node management LIF	Monitor server	Monitoring by SNMP traps

Service	Protocol	Port	Source	Destination	Purpose
SnapMirror	TCP	11104	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	TCP	11105	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
Syslog	UDP	514	Node management LIF	Syslog server	Syslog forward messages

Rules for the HA mediator external security group

The predefined external security group for the Cloud Volumes ONTAP HA mediator includes the following inbound and outbound rules.

Inbound rules

The predefined security group for the HA mediator includes the following inbound rule.

Protocol	Port	Source	Purpose
TCP	3000	CIDR of the Console agent	RESTful API access from the Console agent

Outbound rules

The predefined security group for the HA mediator 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 HA mediator includes the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	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 HA mediator.

Protocol	Port	Destination	Purpose
HTTP	80	IP address of the Console agent on AWS EC2 instance	Download upgrades for the mediator
HTTPS	443	ec2.amazonaws.com	Assist with storage failover

Protocol	Port	Destination	Purpose
UDP	53	ec2.amazonaws.com	Assist with storage failover

Rather than open ports 443 and 53, you can create an interface VPC endpoint from the target subnet to the AWS EC2 service.

Rules for the HA configuration internal security group

The predefined internal security group for a Cloud Volumes ONTAP HA configuration includes the following rules. This security group enables communication between the HA nodes and between the mediator and the nodes.

The Console always creates this security group. You do not have the option to use your own.

Inbound rules

The predefined security group includes the following inbound rules.

Protocol	Port	Purpose
All traffic	All	Communication between the HA mediator and HA nodes

Outbound rules

The predefined security group includes the following outbound rules.

Protocol	Port	Purpose
All traffic	All	Communication between the HA mediator and HA nodes

Rules for the Console agent

View security group rules for the Console agent

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

If you want to use Amazon encryption with Cloud Volumes ONTAP, then you need to set up the AWS Key Management Service (KMS).

Steps

1. Ensure that an active Customer Master Key (CMK) exists.

   The CMK can be an AWS-managed CMK or a customer-managed CMK. It can be in the same AWS account as the NetApp Console and Cloud Volumes ONTAP or in a different AWS account.

   AWS Documentation: Customer Master Keys (CMKs)

2. Modify the key policy for each CMK by adding the IAM role that provides permissions to the Console as a *key user*.

Adding the Identity and Access Management (IAM) role as a key user gives the Console permissions to use the CMK with Cloud Volumes ONTAP.

AWS Documentation: Editing Keys

3. If the CMK is in a different AWS account, complete the following steps:

   a. Go to the KMS console from the account where the CMK resides.

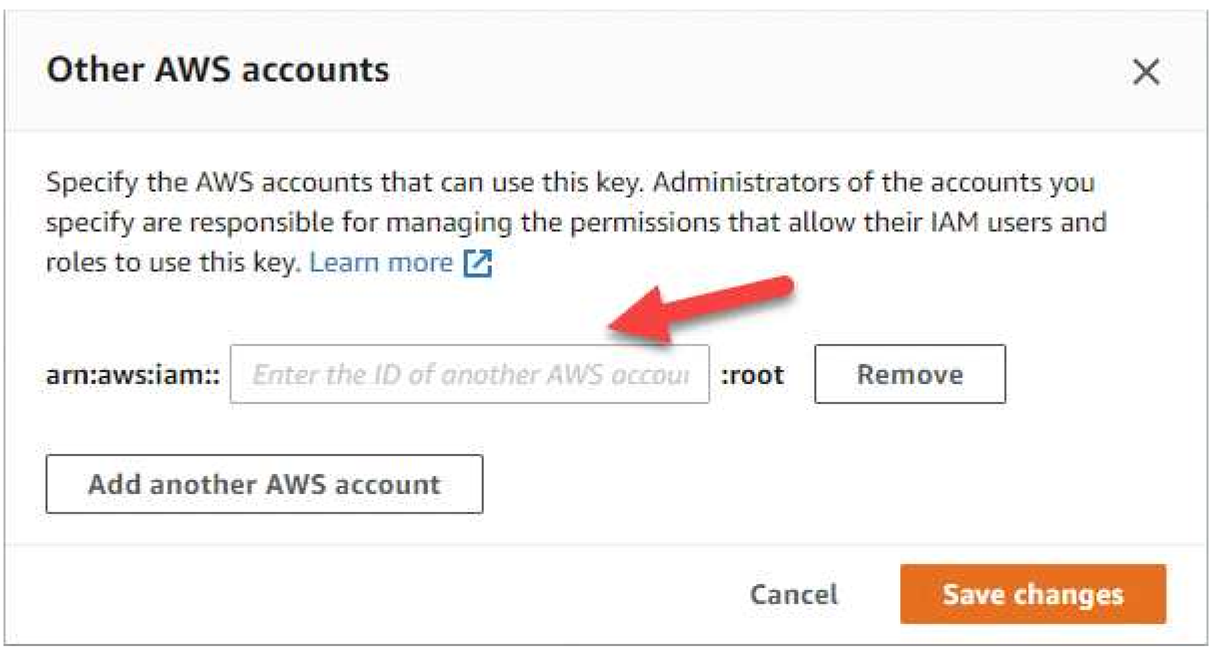
   b. Select the key.

   c. In the **General configuration** pane, copy the ARN of the key.

      You'll need to provide the ARN to the Console when you create the Cloud Volumes ONTAP system.

   d. In the **Other AWS accounts** pane, add the AWS account that provides the Console with permissions.

      Typically, this is the account where the Console is deployed. If the Console is not installed in AWS, use the account for which you provided AWS access keys to the Console.



   e. Now switch to the AWS account that provides the Console with permissions and open the IAM console.

   f. Create an IAM policy that includes the permissions listed below.

   g. Attach the policy to the IAM role or IAM user that provides permissions to the Console.

      The following policy provides the permissions that the Console needs to use the CMK from the external AWS account. Be sure to modify the region and account ID in the "Resource" sections.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

For additional details about this process, refer to the AWS Documentation: Allowing users in other accounts to use a KMS key.

4. If you are using a customer-managed CMK, modify the key policy for the CMK by adding the Cloud Volumes ONTAP IAM role as a *key user*.

   This step is required if you enabled data tiering on Cloud Volumes ONTAP and want to encrypt the data stored in the Amazon Simple Storage Service (Amazon S3) bucket.

You'll need to perform this step *after* you deploy Cloud Volumes ONTAP because the IAM role is created when you create a Cloud Volumes ONTAP system. (Of course, you do have the option to use an existing Cloud Volumes ONTAP IAM role, so it's possible to perform this step before.)

AWS Documentation: Editing Keys

Set up AWS IAM roles for Cloud Volumes ONTAP nodes

AWS Identity and Access management (IAM) roles with the required permissions must be attached to each Cloud Volumes ONTAP node. The same is true for the HA mediator. It's easiest to let the NetApp Console create the IAM roles for you, but you can use your own roles.

This task is optional. When you create a Cloud Volumes ONTAP system, the default option is to let the Console create the IAM roles for you. If your business's security policies require you to create the IAM roles yourself, then follow the steps below.

> ⓘ Providing your own IAM role is required in AWS Secret Cloud. Learn how to deploy Cloud Volumes ONTAP in C2S.

Steps

1. Go to the AWS IAM console.
2. Create IAM policies that include the following permissions:
    - Base policy for Cloud Volumes ONTAP nodes

Standard regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud (US) regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Top Secret regions

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Backup policy for Cloud Volumes ONTAP nodes

  If you plan to use NetApp Backup and Recovery with your Cloud Volumes ONTAP systems, the IAM role for the nodes must include the second policy shown below.

Standard regions

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud (US) regions

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Top Secret regions

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA mediator

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Create an IAM role and attach the policies that you created to the role.

Result

You now have IAM roles that you can select when you create a new Cloud Volumes ONTAP system.

More information

- AWS documentation: Creating IAM policies
- AWS documentation: Creating IAM roles

Set up licensing for Cloud Volumes ONTAP in AWS

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 system.

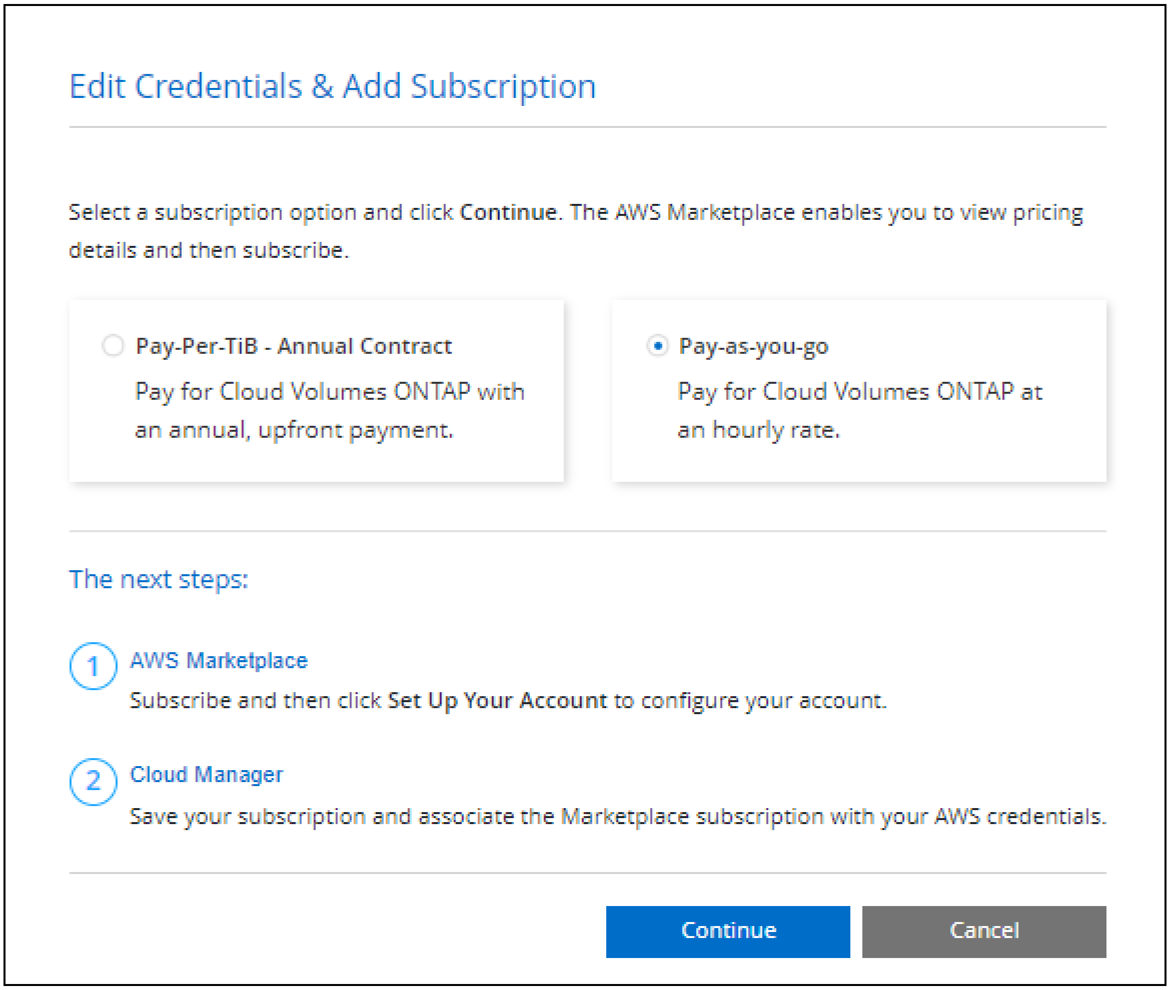
Freemium

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.

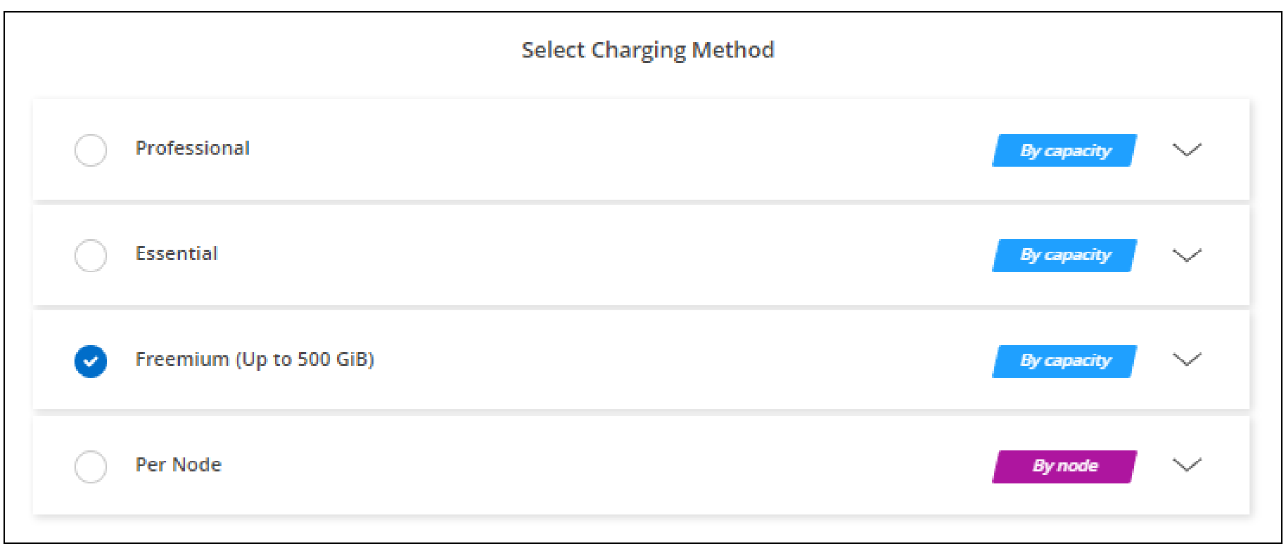
Steps

1. From the left navigation menu of the NetApp Console, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the steps.
   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 AWS 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 the Console, select **Freemium** when you reach the charging methods page.



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

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 or purchase options:

- A license (bring your own license (BYOL)) purchased from NetApp
- An hourly, pay-as-you-go (PAYGO) subscription from the AWS Marketplace
- An annual contract from the AWS Marketplace

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.

NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP.

Steps

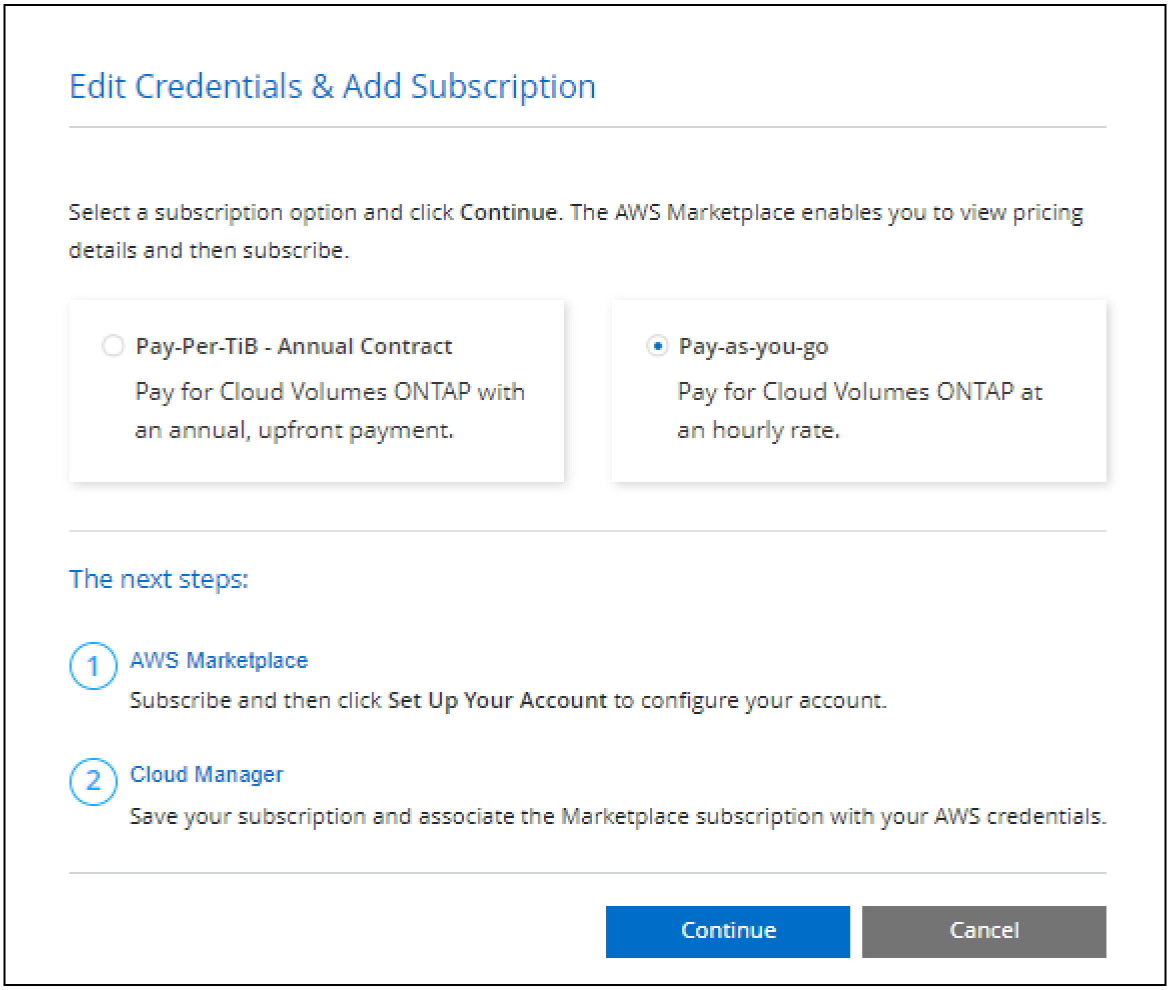
1. Contact NetApp Sales to obtain a license
2. Add your NetApp Support Site account to the Console

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

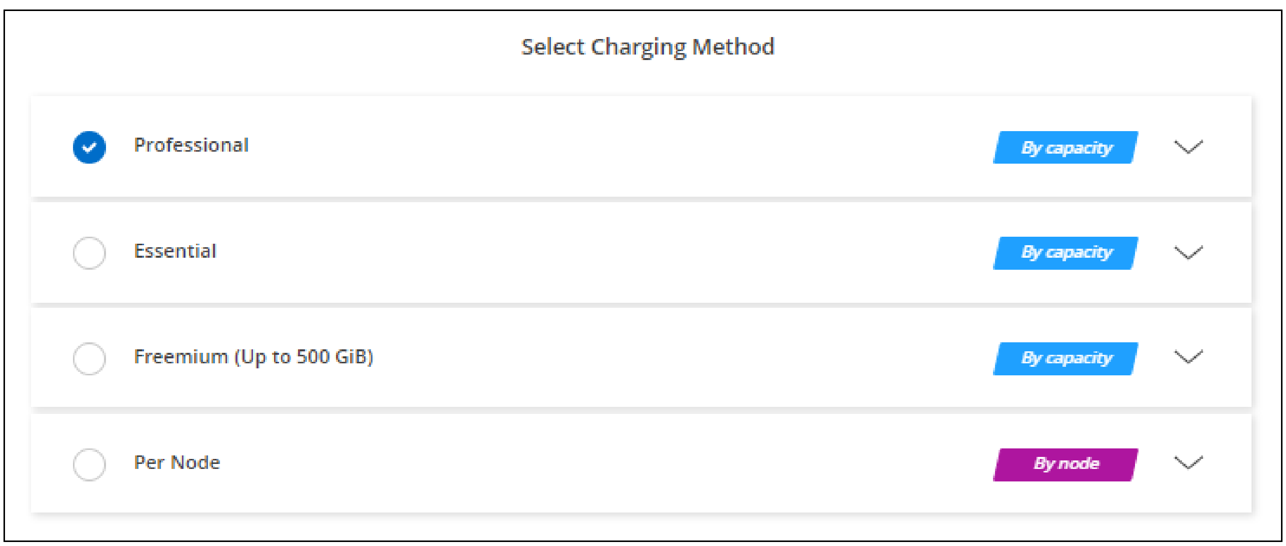
   Your license must be available from the Console before you can use it with Cloud Volumes ONTAP. If needed, you can manually add the license to the Console.

3. On the **Systems** page of the Console, click **Add System** and follow the steps.
   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 AWS 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 the Console, select a capacity-based package when you reach the charging methods page.



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

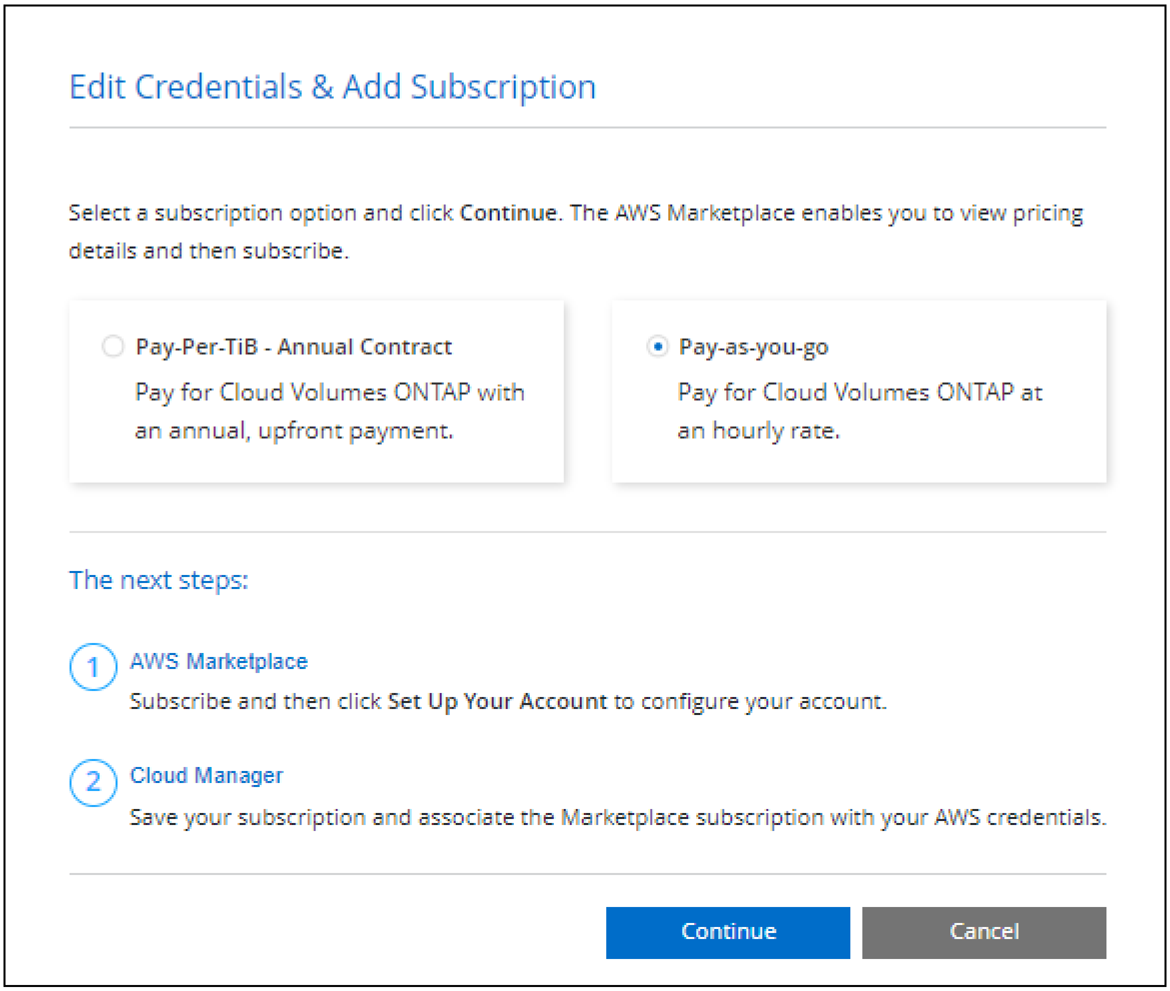
PAYGO subscription

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

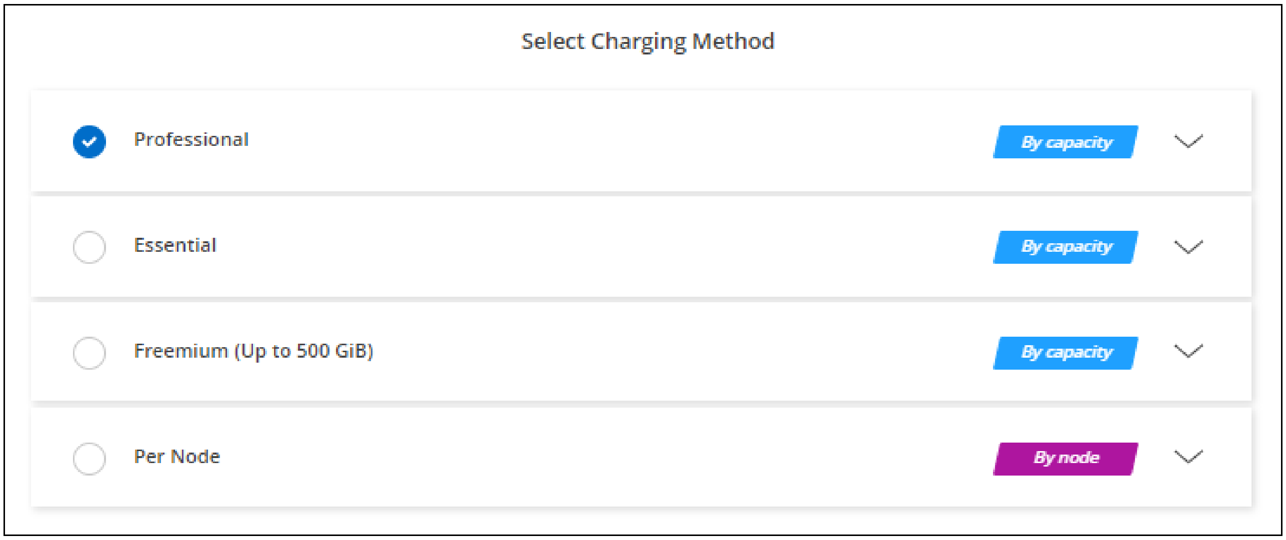
When you create a Cloud Volumes ONTAP system, the Console prompts you to subscribe to the agreement that's available in the AWS Marketplace. That subscription is then associated with the system for charging. You can use that same subscription for additional Cloud Volumes ONTAP systems.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the steps.
   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 AWS Marketplace



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



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

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

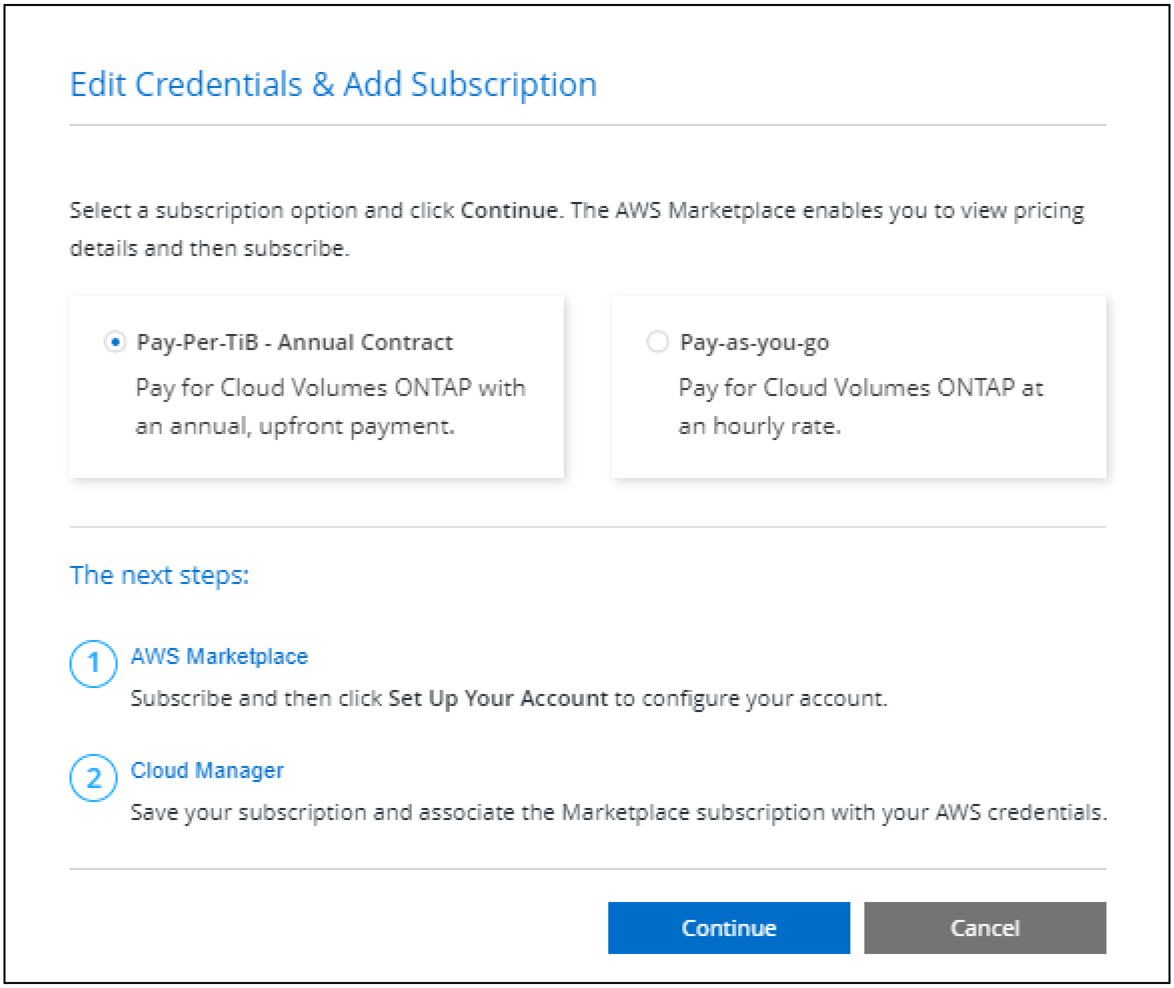
Annual contract

Pay annually by purchasing an annual contract from your cloud provider's marketplace.

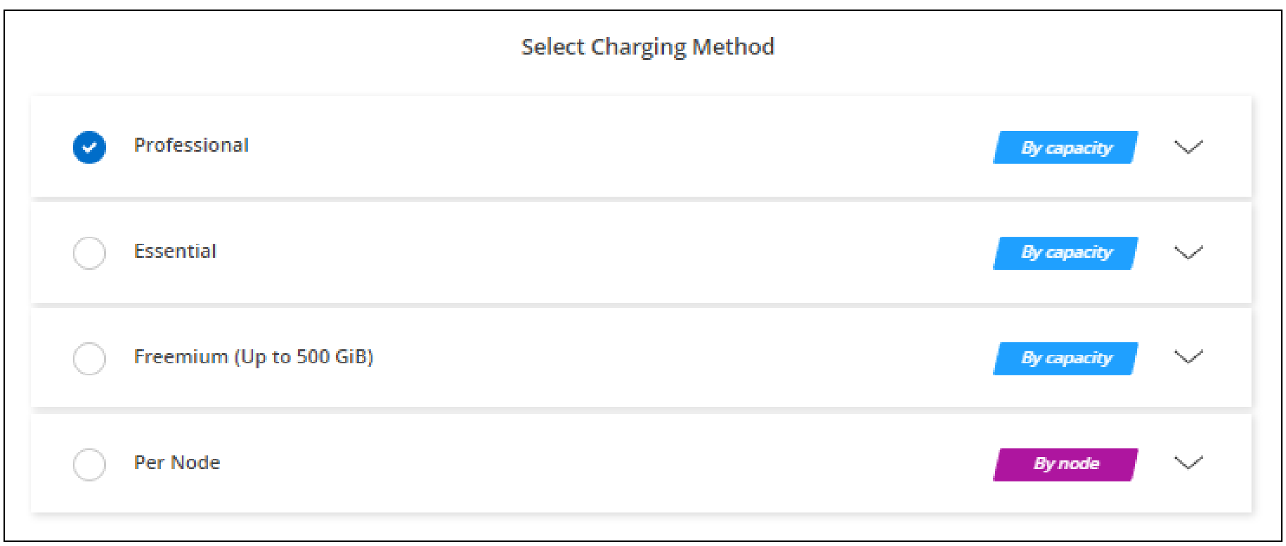
Similar to an hourly subscription, the Console prompts you to subscribe to the annual contract that's available in the AWS Marketplace.

Steps

1. On the **Systems** page, click **Add System** and follow the steps.
    a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the annual contract in the AWS Marketplace.



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



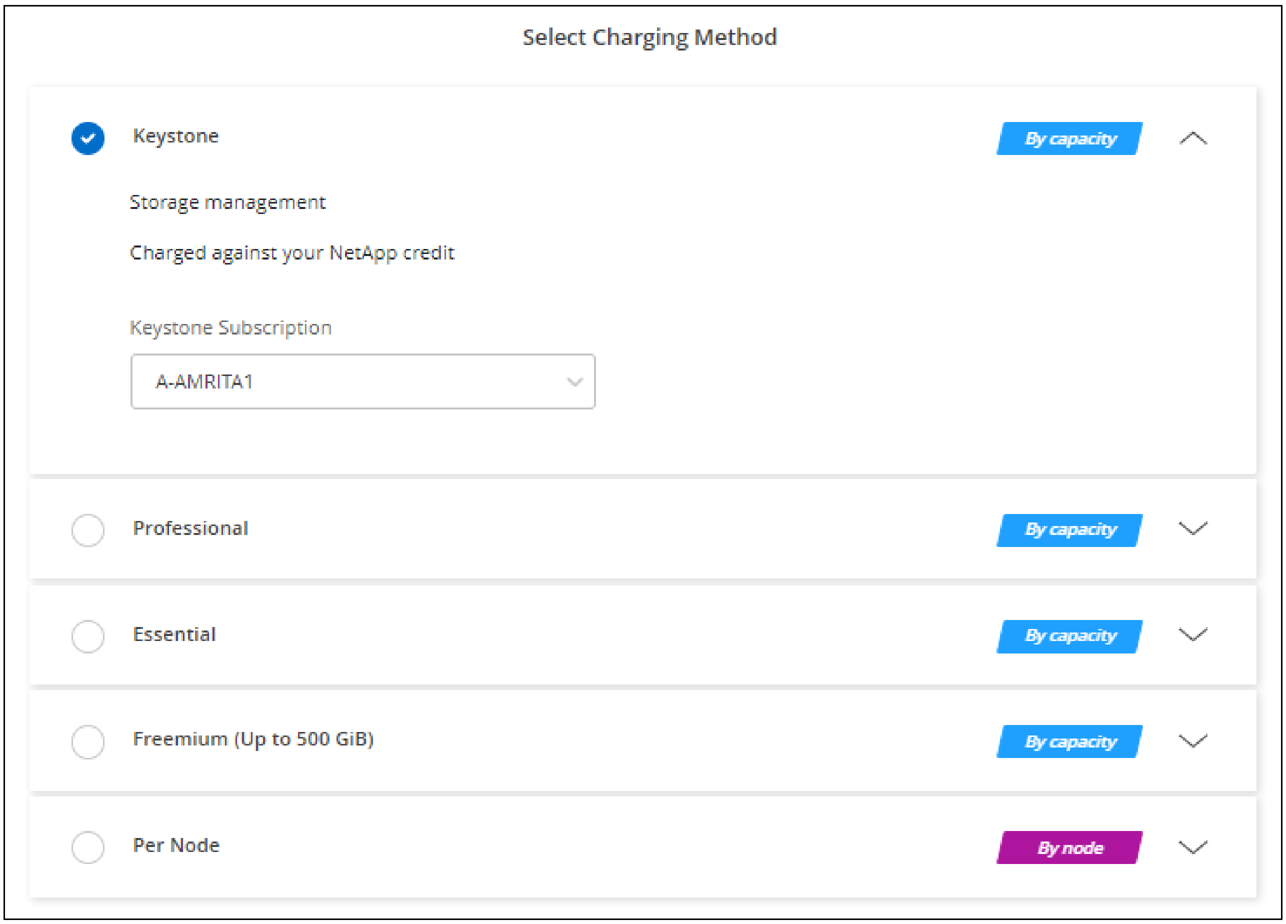
View step-by-step instructions to launch Cloud Volumes ONTAP in AWS.

Keystone Subscription

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

Steps

1. If you don't have a subscription yet, contact NetApp
2. Contact NetApp to authorize your user account with one or more Keystone Subscriptions.
3. After NetApp authorizes your account, link your subscriptions for use with Cloud Volumes ONTAP.
4. On the **Systems** page, click **Add System** and follow the steps.
    a. Select the Keystone Subscription charging method when prompted to choose a charging method.



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

Node-based license

A node-based license is the previous generation license for Cloud Volumes ONTAP. A node-based license could be procured from NetApp (BYOL) and is available for license renewals, only in specific cases. For information, refer to:

- End of availability for node-based licenses
- End of availability of node-based licenses
- Convert a node-based license to a capacity-based license

Deploy Cloud Volumes ONTAP in AWS using quick deployment

You can deploy Cloud Volumes ONTAP in AWS using a quick deployment method for both single node and high availability (HA) configurations. This simplified process reduces deployment steps compared to the advanced method. It also offers more clarity in the workflow by automatically setting default values on a single page and minimizing navigation.

Before you begin

You need the following to add a Cloud Volumes ONTAP system in AWS from the NetApp Console.

- A Console agent that's up and running.
  - You should have a Console agent that is associated with your project or workspace.
  - You should be prepared to leave the Console agent running at all times.
- An understanding of the configuration that you want to use.

  You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, refer to 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.

- DNS and Active Directory for CIFS configurations.

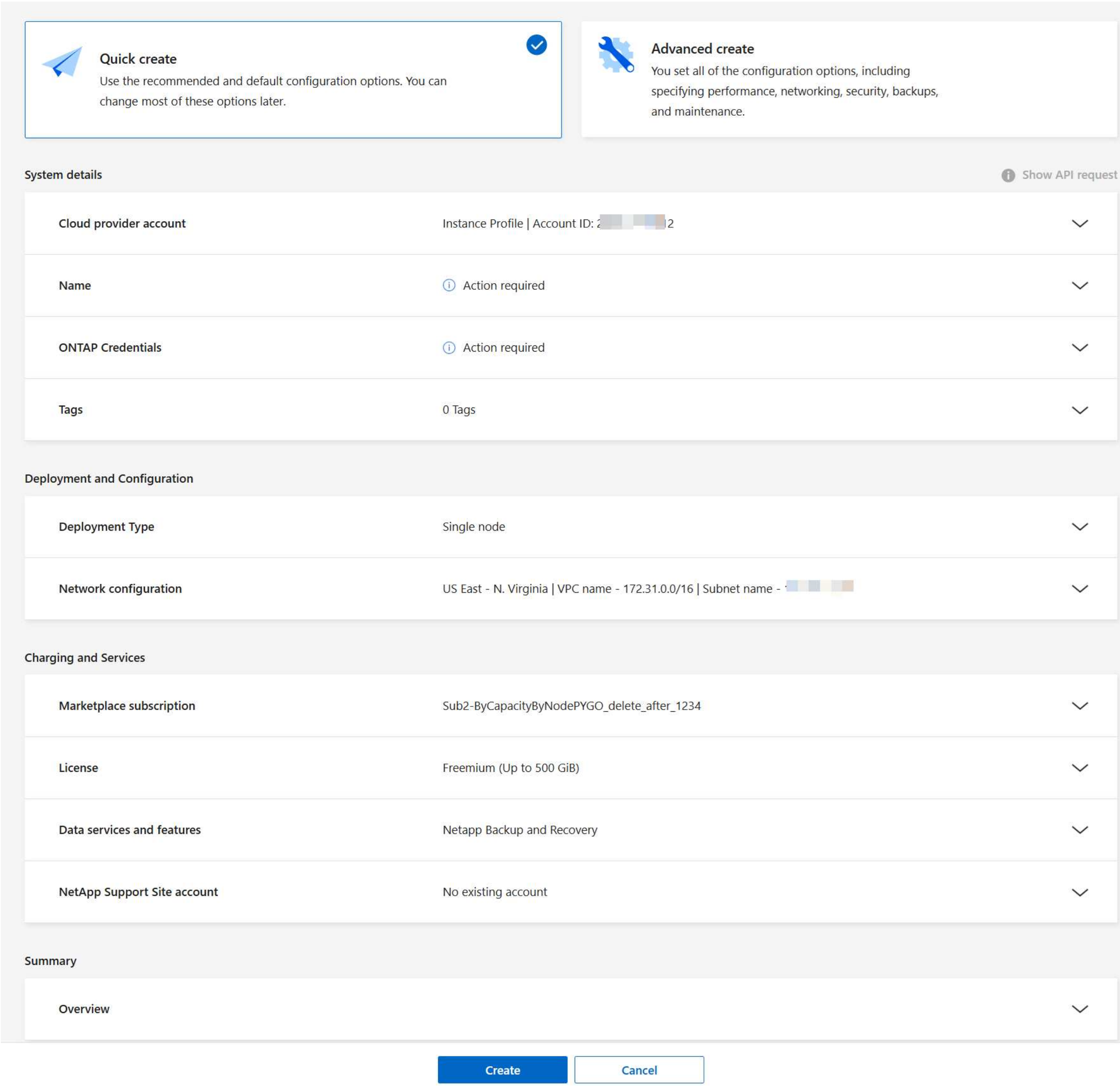
  For details, refer to Networking requirements for Cloud Volumes ONTAP in AWS.

About this task

Immediately after you create the Cloud Volumes ONTAP system, the NetApp Console launches a test instance in the specified VPC to verify connectivity. If successful, the Console immediately terminates the instance and then starts deploying the system. If the Console cannot verify connectivity, creation of the system fails. The test instance is either a `t2.nano` (for default VPC tenancy) or a `m3.medium` (for dedicated VPC tenancy).

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the Canvas page, click **Add System** and follow the prompts.
3. Select **Amazon Web Services** > **Cloud Volumes ONTAP** > **Add new**. The **Quick create** option is selected by default.



system details

1. **Cloud provider account**: The account details are automatically populated based on your selected Console agent. If you have multiple accounts, select the one you want to use. If a Console agent is unavailable, you'll be prompted to create a Console agent.
2. **Name**: The system name. The Console uses the system (cluster) name to name the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.
3. **ONTAP credentials** These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. You can keep the default *admin* user name or change it to a custom user name.
4. **Tags** AWS tags are metadata for your AWS resources. The Console adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. You can add up to 15 tags from the

user interface when creating a Cloud Volumes ONTAP system, and then you can add more after its created. Note that the API does not limit you to four tags when creating a system.
For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.

Deployment and configuration

1. **Deployment type**: Select the deployment type that you want to use, single node, high availability (HA) in a single availability zone (AZ), or HA in a multiple AZ.
2. **Network configuration**: Enter the network information that you recorded in the AWS worksheet.
    a. **AWS region**: By default, the region of the associated cloud account that has VPC with subnet resources is selected.
    b. **VPC**: Enter a VPC for the AWS region with a subnet. If there are no subnets, then the default value for the VPC is selected.
    c. **Subnet**: You can select a subnet for the VPC only for a single node deployment or HA deployment in a single AZ.

High Availability

If you have selected HA configuration, enter the following information:

HA in single AZ

1. **Mediator Access**: Specify the mediator access information. The mediator is a separate instance that monitors the health of the HA pair and provides quorum in case of a failure. Provide the key pair name to enable the mediator instance to connect to the AWS EC2 service, and select the connection method.

HA in multiple AZ

1. **Availability zones and mediator**: Select the availability zones (AZs) for each node and the mediator and the corresponding subnets where you want to deploy the Cloud Volumes ONTAP HA pair.
2. **Floating IPs**: If you chose multiple AZs, specify the floating IP addresses for the NFS and CIFS services and cluster and SVM management. The IP addresses must be outside of the CIDR block for all VPCs in the region. For additional details, refer to AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs.
3. **Mediator Access**: Specify the mediator access information. The mediator is a separate instance that monitors the health of the HA pair and provides quorum in case of a failure. Provide the key pair name to enable the mediator instance to connect to the AWS EC2 service, and select the connection method.
4. **Route Tables**: If you chose multiple AZs, select the route tables that include routes to the floating IP addresses. If you have more than one route table, it is important to select the correct route tables. Otherwise, some clients might not have access to the Cloud Volumes ONTAP HA pair. For more information about route tables, refer to the AWS Documentation: Route Tables.

Charging and Services

1. **Marketplace Subscription**: Select the AWS marketplace subscription you want to use with this Cloud Volumes ONTAP system.
2. **License**: Select the license type you want to use with this Cloud Volumes ONTAP system. You can choose from Professional, Essential, and Premium licenses. For information about different licenses, refer to Learn about Cloud Volumes ONTAP licenses.
3. **Data services and features**: Keep the services enabled or disable the services you don't want to use with Cloud Volumes ONTAP.

    ◦ Learn more about NetApp Classification
    ◦ Learn more about NetApp Backup and Recovery
    ◦ Learn about WORM storage on Cloud Volumes ONTAP

If you want to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

    ◦ **NetApp Support Site account**: If you have multiple accounts, select the one you want to use.

Summary

Check or edit the details you entered, and then click **Create**.

After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the AWS cloud portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

Related links

- Planning your Cloud Volumes ONTAP configuration
- Deploy Cloud Volumes ONTAP in AWS using advanced deployment

Launch Cloud Volumes ONTAP in AWS

You can launch Cloud Volumes ONTAP in a single-system configuration or as an HA pair in AWS. This method provides an advanced deployment experience that offers more configuration options and flexibility than the quick deployment method.

Before you begin

You need the following before you begin.

- A Console agent that's up and running.
    ◦ You should have a Console agent that is associated with your system.
    ◦ You should be prepared to leave the Console agent running at all times.
- An understanding of the configuration that you want to use.

  You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, refer to 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.

- DNS and Active Directory for CIFS configurations.

  For details, refer to Networking requirements for Cloud Volumes ONTAP in AWS.

Launch a single-node Cloud Volumes ONTAP system in AWS

If you want to launch Cloud Volumes ONTAP in AWS, you need to create a new system in the NetApp

Console.

About this task

Immediately after you create the system, the Console launches a test instance in the specified VPC to verify connectivity. If successful, the Console immediately terminates the instance and then starts deploying the Cloud Volumes ONTAP system. If the connectivity can't be verified, system creation fails. The test instance is either a `t2.nano` (for default VPC tenancy) or `m3.medium` (for dedicated VPC tenancy).

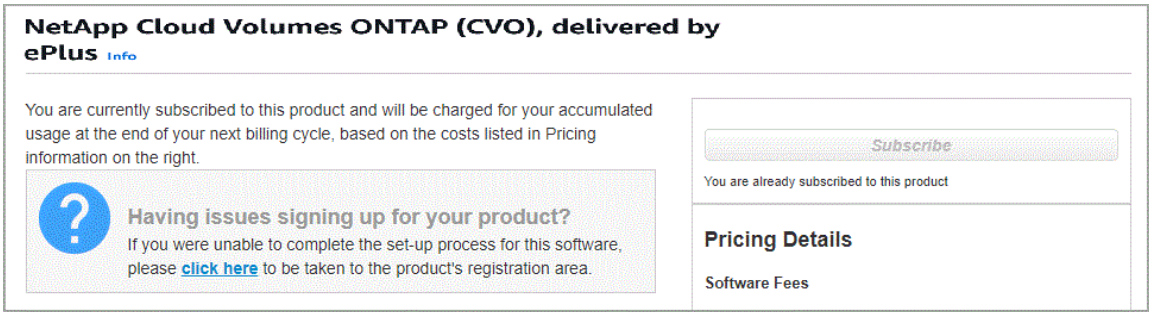
Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the prompts.
3. Select **Amazon Web Services** and **Cloud Volumes ONTAP Single Node**.
4. Select **Advanced create**. Because the **Quick create** mode is selected by default, you might see a message for default values. Click **Continue**.
5. If you're prompted, create a Console agent.
6. **Details and Credentials**: Optionally change the AWS credentials and subscription, enter a system name, add tags if needed, and then enter a password.

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

Field	Description
System Name	The Console uses the system name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Add tags	AWS tags are metadata for your AWS resources. The Console adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. You can add up to four tags from the user interface when creating a system, and then you can add more after it's created. Note that the API does not limit you to four tags when creating a system. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.
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 ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Credentials	Choose the AWS credentials associated with the account where you want to deploy this system. You can also associate the AWS marketplace subscription to use with this Cloud Volumes ONTAP system. Click **Add Subscription** to associate the selected credentials with a new AWS marketplace subscription. The subscription can be for an annual contract or to pay for Cloud Volumes ONTAP at an hourly rate. Learn how to add additional AWS credentials to NetApp Console.

If multiple IAM users work in the same AWS account, then each user needs to subscribe. After the first user subscribes, the AWS marketplace informs subsequent users that they're already subscribed, as shown in the image below. While a subscription is in place for the AWS *account*, each IAM user needs to associate themselves with that subscription. If you see the message shown below, click the **click here** link to go to the Console website and complete the process.



7. **Services**: Keep the services enabled or disable the individual services that you don't want to use with Cloud Volumes ONTAP.
   - Learn more about NetApp Data Classification
   - Learn more about NetApp Backup and Recovery

   If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

8. **Location & Connectivity**: Enter the network information that you recorded in the AWS worksheet.

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

Field	Description
VPC	If you have an AWS Outpost, you can deploy a single node Cloud Volumes ONTAP system in that Outpost by selecting the Outpost VPC. The experience is the same as any other VPC that resides in AWS.
Generated security group	If you let the Console generate the security group for you, you need to choose how you'll allow traffic: • If you choose **Selected VPC only**, the source for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Console agent resides. This is the recommended option. • If you choose **All VPCs**, the source for inbound traffic is the 0.0.0.0/0 IP range.
Use existing security group	If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.

9. **Data Encryption**: Choose no data encryption or AWS-managed encryption.

   For AWS-managed encryption, you can choose a different Customer Master Key (CMK) from your account or another AWS account.

You can't change the AWS data encryption method after you create a Cloud Volumes ONTAP system.

Learn how to set up the AWS KMS for Cloud Volumes ONTAP.

Learn more about supported encryption technologies.

10. **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.
11. **Cloud Volumes ONTAP Configuration** (annual AWS marketplace contract only): Review the default configuration and click **Continue** or click **Change Configuration** to select your own configuration.

    If you keep the default configuration, then you only need to specify a volume and then review and approve the configuration.
12. **Preconfigured Packages**: Select one of the packages to quickly launch Cloud Volumes ONTAP, or click **Change Configuration** to select your own configuration.

    If you choose one of the packages, then you only need to specify a volume and then review and approve the configuration.
13. **IAM Role**: It's best to keep the default option to let the Console create the role for you.

    If you prefer to use your own policy, it must meet policy requirements for Cloud Volumes ONTAP nodes.
14. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select an instance type and the instance tenancy.

    If a newer Release Candidate, General Availability, or patch release is available for the selected version, then the Console updates the system to that version when creating the system. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another—for example, from 9.13 to 9.14.
15. **Underlying Storage Resources**: Choose a disk type, configure the underlying storage, and choose whether to keep data tiering enabled.

    Note the following:

    - The disk type is for the initial volume (and aggregate). You can choose a different disk type for subsequent volumes (and aggregates).
    - If you choose a gp3 or io1 disk, the Console uses the Elastic Volumes feature in AWS to automatically increase the underlying storage disk capacity as needed. 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.
    - If you choose a gp2 or st1 disk, you can select a disk size for all disks in the initial aggregate and for any additional aggregates that the Console creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.
    - 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 how data tiering works.

16. **Write Speed & WORM**:

    a. Choose **Normal** or **High** write speed, if desired.

       Learn more about write speed.

    b. Activate write once, read many (WORM) storage, if desired.

       WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

       Learn more about WORM storage.

    c. If you activate WORM storage, select the retention period.

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

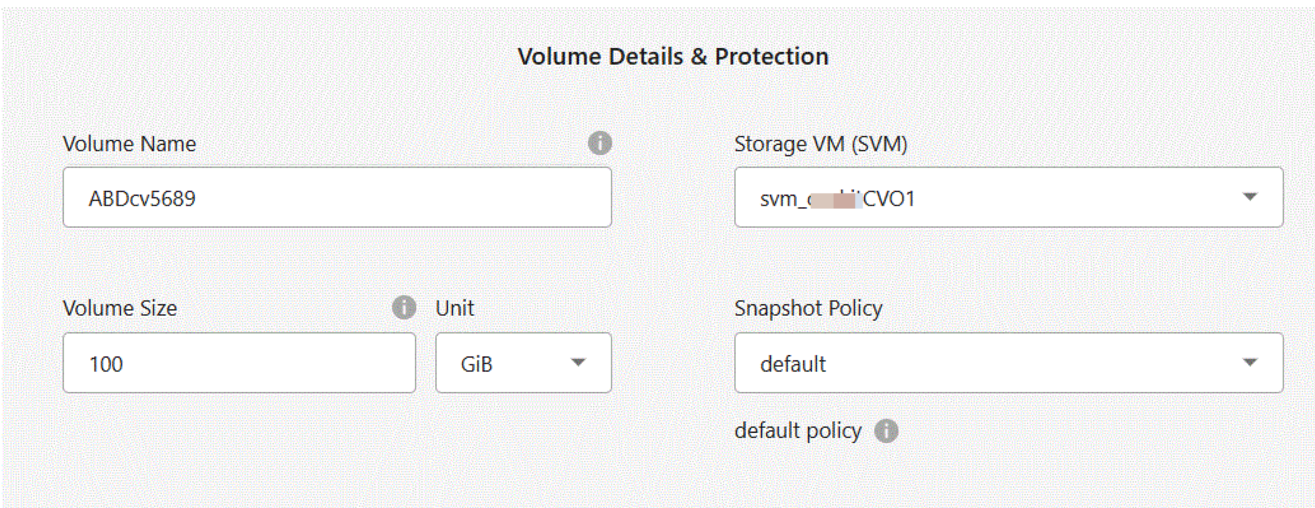
    Learn about supported client protocols and versions.

    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, the Console 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.

Field	Description
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, the Console 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 first page of the volume creation wizard:



18. **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.

Field	Description
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field.
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. Refer to the NetApp Console 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.

19. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and edit the volume tiering policy, if needed.

    For more information, refer to Understanding volume usage profiles, Data tiering overview, and KB: What Inline Storage Efficiency features are supported with CVO?

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

    a. Review details about the configuration.

    b. Click **More information** to review details about support and the AWS resources that the Console will purchase.

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

    d. Click **Go**.

Result

The Console launches the Cloud Volumes ONTAP instance. You can track the progress on the **Audit** page.

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

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

> After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the AWS cloud portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

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 ONTAP System Manager or the ONTAP CLI.

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

Launch a Cloud Volumes ONTAP HA pair in AWS

If you want to launch a Cloud Volumes ONTAP HA pair in AWS, you need to create an HA system in the Console.

Limitation

At this time, HA pairs are not supported with AWS Outposts.

About this task

Immediately after you create the Cloud Volumes ONTAP system, the Console launches a test instance in the specified VPC to verify connectivity. If successful, the Console immediately terminates the instance and then starts deploying the Cloud Volumes ONTAP system. If the connectivity can't be verified, system creation fails. The test instance is either a `t2.nano` (for default VPC tenancy) or `m3.medium` (for dedicated VPC tenancy).

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the prompts.
3. Select **Amazon Web Services** and **Cloud Volumes ONTAP HA**.

   Some AWS Local Zones are available.

   Before you can use AWS Local Zones, you must enable Local Zones and create a subnet in the Local Zone in your AWS account. Follow the **Opt in to an AWS Local Zone** and **Extend your Amazon VPC to the Local Zone** steps in the AWS tutorial "Get Started Deploying Low Latency Applications with AWS Local Zones.

   If you are running the Console agent 3.9.36 or below, you need to add the `DescribeAvailabilityZones` permission to the AWS role in the AWS EC2 console.

4. **Details and Credentials**: Optionally change the AWS credentials and subscription, enter a system name, add tags if needed, and then enter a password.

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

Field	Description
System Name	The Console uses the system name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Add tags	AWS tags are metadata for your AWS resources. The Console adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. You can add up to four tags from the user interface when creating a system, and then you can add more after it's created. Note that the API does not limit you to four tags when creating a system. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 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 ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Credentials	Choose the AWS credentials and marketplace subscription to use with this Cloud Volumes ONTAP system. Click **Add Subscription** to associate the selected credentials with a new AWS marketplace subscription. The subscription can be for an annual contract or to pay for Cloud Volumes ONTAP at an hourly rate. If you purchased a license directly from NetApp (bring your own license (BYOL)), then an AWS subscription isn't required. NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP. Learn how to add additional AWS credentials to the Console.

> If multiple IAM users work in the same AWS account, then each user needs to subscribe. After the first user subscribes, the AWS marketplace informs subsequent users that they're already subscribed, as shown in the image below. While a subscription is in place for the AWS *account*, each IAM user needs to associate themselves with that subscription. If you see the message shown below, click the **click here** link to go to the Console website and complete the process.

5. **Services**: Keep the services enabled or disable the individual services that you don't want to use with this Cloud Volumes ONTAP system.
   - Learn more about NetApp Data Classification
   - Learn more about Backup and Recovery

   > If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

6. **HA Deployment Models**: Choose an HA configuration.

   For an overview of the deployment models, refer to Cloud Volumes ONTAP HA for AWS.

7. **Location and Connectivity** (single availability zone (AZ)) or **Region & VPC** (multiple AZs): Enter the network information that you recorded in the AWS worksheet.

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

Field	Description
Generated security group	If you let the Console generate the security group for you, you need to choose how you'll allow traffic: • If you choose **Selected VPC only**, the source for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Console agent resides. This is the recommended option. • If you choose **All VPCs**, the source for inbound traffic is the 0.0.0.0/0 IP range.
Use existing security group	If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.

8. **Connectivity and SSH Authentication**: Choose connection methods for the HA pair and the mediator.
9. **Floating IPs**: If you chose multiple AZs, specify the floating IP addresses.

   The IP addresses must be outside of the CIDR block for all VPCs in the region. For additional details, refer to AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs.

10. **Route Tables**: If you chose multiple AZs, select the route tables that should include routes to the floating IP addresses.

    If you have more than one route table, it is very important to select the correct route tables. Otherwise, some clients might not have access to the Cloud Volumes ONTAP HA pair. For more information about route tables, refer to the AWS Documentation: Route Tables.

11. **Data Encryption**: Choose no data encryption or AWS-managed encryption.

    For AWS-managed encryption, you can choose a different Customer Master Key (CMK) from your account or another AWS account.

    > You can't change the AWS data encryption method after you create a Cloud Volumes ONTAP system.

    Learn how to set up the AWS KMS for Cloud Volumes ONTAP.

    Learn more about supported encryption technologies.

12. **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.
13. **Cloud Volumes ONTAP Configuration** (annual AWS Marketplace contract only): Review the default configuration and click **Continue** or click **Change Configuration** to select your own configuration.

    If you keep the default configuration, then you only need to specify a volume and then review and approve the configuration.

14. **Preconfigured Packages** (hourly or BYOL only): Select one of the packages to quickly launch Cloud Volumes ONTAP, or click **Change Configuration** to select your own configuration.

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

15. **IAM Role**: It's best to keep the default option to let the Console create the role for you.

    If you prefer to use your own policy, it must meet policy requirements for Cloud Volumes ONTAP nodes and the HA mediator.

16. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select an instance type and the instance tenancy.

    > If a newer Release Candidate, General Availability, or patch release is available for the selected version, then the Console updates the system to that version when creating the system. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another—for example, from 9.13 to 9.14.

17. **Underlying Storage Resources**: Choose a disk type, configure the underlying storage, and choose whether to keep data tiering enabled.

    Note the following:

    - The disk type is for the initial volume (and aggregate). You can choose a different disk type for subsequent volumes (and aggregates).
    - If you choose a gp3 or io1 disk, the Console uses the Elastic Volumes feature in AWS to automatically increase the underlying storage disk capacity as needed. 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.
    - If you choose a gp2 or st1 disk, you can select a disk size for all disks in the initial aggregate and for any additional aggregates that the Console creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.
    - 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 how data tiering works.

18. **Write Speed & WORM**:

    a. Choose **Normal** or **High** write speed, if desired.

       Learn more about write speed.

    b. Activate write once, read many (WORM) storage, if desired.

       WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

       Learn more about WORM storage.

    c. If you activate WORM storage, select the retention period.

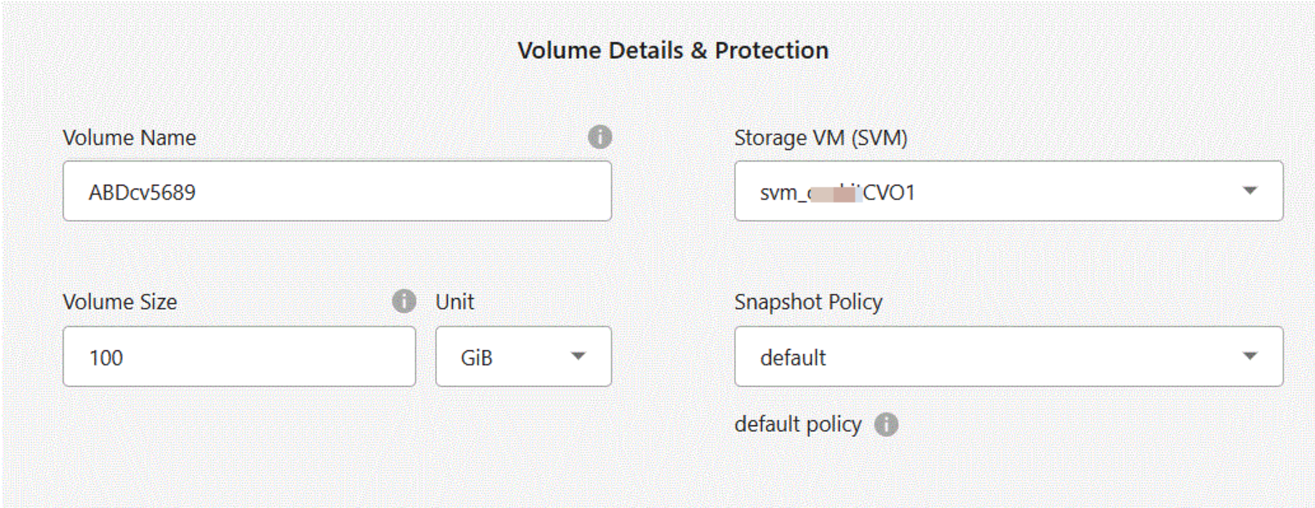
19. **Create Volume**: Enter details for the new volume or click **Skip**.

    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, the Console 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, the Console 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 first page of the volume creation wizard:



20. **CIFS Setup**: If you selected 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. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field.
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. Refer to the NetApp Console 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.

21. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and edit the volume tiering policy, if needed.

    For more information, refer to Choose a volume usage profile and Data tiering overview.

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

a. Review details about the configuration.

b. Click **More information** to review details about support and the AWS resources that the Console will purchase.

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

d. Click **Go**.

Result

The Console launches the Cloud Volumes ONTAP HA pair. You can track the progress on the **Audit** page.

If you experience any issues launching the HA pair, review the failure message. You can also select the system 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 ONTAP System Manager or the ONTAP CLI.

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

> After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the AWS cloud portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

Related links

- Planning your Cloud Volumes ONTAP configuration
- Deploy Cloud Volumes ONTAP in AWS using quick deployment

Deploy Cloud Volumes ONTAP in AWS Secret Cloud or AWS Top Secret Cloud

Similar to a standard AWS region, you can use the NetApp Console in AWS Secret Cloud and in AWS Top Secret Cloud to deploy Cloud Volumes ONTAP, which provides enterprise-class features for your cloud storage. AWS Secret Cloud and Top Secret Cloud are closed regions specific to the U.S. Intelligence Community; the instructions on this page only apply to AWS Secret Cloud and Top Secret Cloud region users.

Before you begin

Before you get started, review the supported versions in AWS Secret Cloud and Top Secret Cloud, and learn about private mode in the Console.

- Review the following supported versions in AWS Secret Cloud and Top Secret Cloud:
  - Cloud Volumes ONTAP 9.12.1 P2
  - Version 3.9.32 of the Console agent

    The Console agent is required to deploy and manage Cloud Volumes ONTAP in AWS. You'll log in to the Console from the software that gets installed on the instance of the Console agent. The SaaS website for the Console isn't supported in AWS Secret Cloud and Top Secret Cloud.

- Learn about private mode

  In AWS Secret Cloud and Top Secret Cloud, the Console operates in *private mode*. In private mode, there is no connectivity to the SaaS layer from the Console. You can access the Console through a local a web-based application that can access the Console agent.

  To learn more about how private mode works, refer to the private deployment mode in the Console.

Step 1: Set up your networking

Set up your AWS networking so Cloud Volumes ONTAP can operate properly.

Steps

1. Choose the VPC and subnets in which you want to launch the instance of the Console agent and Cloud Volumes ONTAP instances.
2. Ensure that your VPC and subnets will support connectivity between the Console agent and Cloud Volumes ONTAP.
3. Set up a VPC endpoint to the Amazon Simple Storage Service (Amazon S3) service.

   A VPC endpoint is required if you want to tier cold data from Cloud Volumes ONTAP to low-cost object storage.

Step 2: Set up permissions

Set up IAM policies and roles that provide the Console agent and Cloud Volumes ONTAP with the permissions that they need to perform actions in the AWS Secret Cloud or Top Secret Cloud.

You need an IAM policy and IAM role for each of the following:

- The instance of the Console agent
- Cloud Volumes ONTAP instances
- For HA pairs, the Cloud Volumes ONTAP HA mediator instance (if you want to deploy HA pairs)

Steps

1. Go to the AWS IAM console and click **Policies**.
2. Create a policy for the instance of the Console agent.

> You create these policies to support the S3 buckets in your AWS environment. While creating the buckets later, ensure that the bucket names are prefixed with `fabric-pool-`. This requirement applies to both the AWS Secret Cloud and Top Secret Cloud regions.

Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Top Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
```

```
"ec2:RevokeSecurityGroupIngress",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateNetworkInterface",
"ec2:DescribeNetworkInterfaces",
"ec2:DeleteNetworkInterface",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeDhcpOptions",
"ec2:CreateSnapshot",
"ec2:DeleteSnapshot",
"ec2:DescribeSnapshots",
"ec2:GetConsoleOutput",
"ec2:DescribeKeyPairs",
"ec2:DescribeRegions",
"ec2:DeleteTags",
"ec2:DescribeTags",
"cloudformation:CreateStack",
"cloudformation:DeleteStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:ValidateTemplate",
"iam:PassRole",
"iam:CreateRole",
"iam:DeleteRole",
"iam:PutRolePolicy",
"iam:ListInstanceProfiles",
"iam:CreateInstanceProfile",
"iam:DeleteRolePolicy",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:DeleteInstanceProfile",
"s3:GetObject",
"s3:ListBucket",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListAllMyBuckets",
"kms:List*",
"kms:Describe*",
"ec2:AssociateIamInstanceProfile",
"ec2:DescribeIamInstanceProfileAssociations",
"ec2:DisassociateIamInstanceProfile",
"ec2:DescribeInstanceAttribute",
"ec2:CreatePlacementGroup",
"ec2:DeletePlacementGroup"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
```

```
}
```

3. Create a policy for Cloud Volumes ONTAP.

Secret regions

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Top Secret regions

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

For HA pairs, if you plan to deploy a Cloud Volumes ONTAP HA pair, create a policy for the HA mediator.

```json
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Create IAM roles with the role type Amazon EC2 and attach the policies that you created in the previous steps.

   Create the role:

   Similar to the policies, you should have one IAM role for the Console agent and one for the Cloud Volumes ONTAP nodes.
   For HA pairs: Similar to the policies, you should have one IAM role for the Console agent, one for the Cloud Volumes ONTAP nodes, and one for the HA mediator (if you want to deploy HA pairs).

   Select the role:

   You must select the Console agent IAM role when you launch the instance of the Console agent. You can select the IAM roles for Cloud Volumes ONTAP when you create a Cloud Volumes ONTAP system from the Console.
   For HA pairs, you can select the IAM roles for Cloud Volumes ONTAP and the HA mediator when you create a Cloud Volumes ONTAP system.

Step 3: Set up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, ensure that requirements are met for the AWS Key Management Service (KMS).

Steps

1. Ensure that an active Customer Master Key (CMK) exists in your account or in another AWS account.

   The CMK can be an AWS-managed CMK or a customer-managed CMK.

2. If the CMK is in an AWS account separate from the account where you plan to deploy Cloud Volumes ONTAP, then you need to obtain the ARN of that key.

   You need to provide the ARN to the Console when you create the Cloud Volumes ONTAP system.

3. Add the IAM role for the instance to the list of key users for a CMK.

   This gives the Console permissions to use the CMK with Cloud Volumes ONTAP.

Step 4: Install the Console agent and set up the Console

Before you can start using the Console to deploy Cloud Volumes ONTAP in AWS, you must install and set up the Console agent. It enables the Console to manage resources and processes within your public cloud environment (this includes Cloud Volumes ONTAP).

Steps

1. Obtain a root certificate signed by a certificate authority (CA) in the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. Consult your organization's policies and procedures for obtaining the certificate.

   > For AWS Secret Cloud regions, you should upload the `NSS Root CA 2` certificate, and for Top Secret Cloud, the `Amazon Root CA 4` certificate. Ensure that you upload only these certificates and not the entire chain. The file for the certificate chain is large, and the upload can fail. If you have additional certificates, you can upload them later, as described in the next step.

   You need to upload the certificate during the setup process. The Console uses the trusted certificate when sending requests to AWS over HTTPS.

2. Launch the instance of the Console agent:

   a. Go to the AWS Intelligence Community Marketplace page for the Console.

   b. On the Custom Launch tab, choose the option to launch the instance from the EC2 console.

   c. Follow the prompts to configure the instance.

      Note the following as you configure the instance:

      - We recommend t3.xlarge.
      - You must choose the IAM role that you created when you set up permissions.
      - You should keep the default storage options.
      - The required connection methods for the Console agent are as follows: SSH, HTTP, and HTTPS.

3. Set up the Console from a host that has a connection to the instance:

   a. Open a web browser and enter https://*ipaddress* where *ipaddress* is the IP address of the Linux host where you installed the Console agent.

   b. Specify a proxy server for connectivity to AWS services.

   c. Upload the certificate that you obtained in step 1.

   d. Follow the prompts to set up a new system.

      - **System Details**: Enter a name for the Console agent and your company name.
      - **Create Admin User**: Create the admin user for the system.

        This user account runs locally on the system. There's no connection to the auth0 service available through the Console.

      - **Review**: Review the details, accept the license agreement, and then select **Set Up**.

e. To complete installation of the CA-signed certificate, restart the Console agent instance from the EC2 console.

4. After the Console agent restarts, log in using the administrator user account that you created in the Setup wizard.

Step 5: (optional) Install a private mode certificate

This step is optional for AWS Secret Cloud and Top Secret Cloud regions, and is required only if you have additional certificates apart from the root certificates that you installed in the previous step.

Steps

1. List existing installed certificates.
   a. To collect the occm container docker id (identified name “ds-occm-1”), run the following command:

   ```
   docker ps
   ```

   b. To get inside occm container, run the following command:

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   c. To collect the password from “TRUST_STORE_PASSWORD” environment variable, run the following command:

   ```
   env
   ```

   d. To list all installed certificates in truststore, run the following command and use the password collected in the previous step:

   ```
   keytool -list -v -keystore occm.truststore
   ```

2. Add a certificate.
   a. To collect occm container docker id (identified name “ds-occm-1”), run the following command:

   ```
   docker ps
   ```

   b. To get inside occm container, run the following command:

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   Save the new certificate file inside.

   c. To collect the password from “TRUST_STORE_PASSWORD” environment variable, run the following command:

```
env
```

d. To add the certificate to the truststore, run the following command and use the password from the previous step:

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. To check that the certificate installed, run the following command:

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. To exit occm container, run the following command:

```
exit
```

g. To reset occm container, run the following command:

```
docker restart <docker-id>
```

Step 6: Add a license to the Console

If you purchased a license from NetApp, you need to add it to the Console, so that you can select the license when you create a new Cloud Volumes ONTAP system. These licenses remain unassigned until you associate them with a new Cloud Volumes ONTAP system.

Steps

1. From the left navigation menu, select **Licenses and subscriptions**.
2. On the **Cloud Volumes ONTAP** panel, select **View**.
3. On the **Cloud Volumes ONTAP** tab, select **Licenses > Node Based Licenses**.
4. Click **Unassigned**.
5. Click **Add Unassigned Licenses**.
6. Enter the serial number of the license or upload the license file.
7. If you don't have the license file yet, you'll need to manually upload the license file from netapp.com.
   a. Go to the NetApp License File Generator and log in using your NetApp Support Site credentials.
   b. Enter your password, choose your product, enter the serial number, confirm that you have read and accepted the privacy policy, and then click **Submit**.
   c. Choose whether you want to receive the serialnumber.NLF JSON file through email or direct download.

8. Click **Add License**.

Result

The Console adds the license as unassigned until you associate it with a new Cloud Volumes ONTAP system. You can see the license on the left navigation menu under **Licenses and subscriptions > Cloud Volumes ONTAP > View > Licenses**.

Step 7: Launch Cloud Volumes ONTAP from the Console

You can launch Cloud Volumes ONTAP instances in AWS Secret Cloud and Top Secret Cloud by creating new systems in the Console.

Before you begin

For HA pairs, a key pair is required to enable key-based SSH authentication to the HA mediator.

Steps

1. On the **Systems** page, click **Add System**.
2. Under **Create**, select Cloud Volumes ONTAP.

   For HA: Under **Create**, select Cloud Volumes ONTAP or Cloud Volumes ONTAP HA.

3. Complete the steps in the wizard to launch the Cloud Volumes ONTAP system.

   > While making selections through the wizard, do not select **Data Sense & Compliance** and **Backup to Cloud** under **Services**. Under **Preconfigured Packages**, select **Change Configuration** only, and ensure that you haven't selected any other option. Preconfigured packages aren't supported in AWS Secret Cloud and Top Secret Cloud regions, and if selected, your deployment will fail.

Notes for deploying Cloud Volumes ONTAP HA in multiple Availability Zones

Note the following as you complete the wizard for HA pairs.

- You should configure a transit gateway when you deploy Cloud Volumes ONTAP HA in multiple Availability Zones (AZs). For instructions, refer to Set up an AWS transit gateway.
- Deploy the configuration as the following because only two AZs were available in the AWS Top Secret Cloud at the time of publication:
  - Node 1: Availability Zone A
  - Node 2: Availability Zone B
  - Mediator: Availability Zone A or B

Notes for deploying Cloud Volumes ONTAP in both single and HA nodes

Note the following as you complete the wizard:

- You should leave the default option to use a generated security group.

  The predefined security group includes the rules that Cloud Volumes ONTAP needs to operate successfully. If you have a requirement to use your own, you can refer to the security group section below.

- You must choose the IAM role that you created when preparing your AWS environment.
- The underlying AWS disk type is for the initial Cloud Volumes ONTAP volume.

You can choose a different disk type for subsequent volumes.

- The performance of AWS disks is tied to disk size.

  You should choose the disk size that gives you the sustained performance that you need. Refer to the AWS documentation for more details about EBS performance.

- The disk size is the default size for all disks on the system.

  > If you need a different size later, you can use the Advanced allocation option to create an aggregate that uses disks of a specific size.

Result

The Cloud Volumes ONTAP instance is launched. You can track the progress in the **Audit** page.

Step 8: Install security certificates for data tiering

You need to manually install security certificates for enabling data tiering in AWS Secret Cloud and Top Secret Cloud regions.

Before you begin

1. Create S3 buckets.

   > Ensure that the bucket names are prefixed with `fabric-pool-`. For example `fabric-pool-testbucket`.

2. Keep the root certificates that you installed in `step 4` handy.

Steps

1. Copy the text from the root certificates that you installed in `step 4`.
2. Securely connect to the Cloud Volumes ONTAP system by using the CLI.
3. Install the root certificates. You might need to press the `ENTER` key multiple times:

   ```
   security certificate install -type server-ca -cert-name <certificate-name>
   ```

4. When prompted, enter the entire copied text, including and from `----- BEGIN CERTIFICATE -----` to `----- END CERTIFICATE -----`.
5. Keep a copy of the CA-signed digital certificate for future reference.
6. Retain the CA name and certificate serial number.
7. Configure the object store for AWS Secret Cloud and Top Secret Cloud regions: `set -privilege advanced -confirmations off`
8. Run this command to configure the object store.

> All Amazon Resource Names (ARNs) should be suffixed with `-iso-b`, such as `arn:aws-iso-b`. For example, if a resource requires an ARN with a region, for Top Secret Cloud, use the naming convention as `us-iso-b` for the `-server` flag. For AWS Secret Cloud, use `us-iso-b-1`.

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. Verify that the object store was created successfully: `storage aggregate object-store show -instance`
10. Attach the object store to the aggregate. This should be repeated for every new aggregate: `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

Get started in Microsoft Azure

Learn about Cloud Volumes ONTAP deployment options in Azure

NetApp provides two options for deploying Cloud Volumes ONTAP on Azure. Cloud Volumes ONTAP traditionally relies on the NetApp Console for deployment and orchestration. Beginning with Cloud Volumes ONTAP 9.16.1, you can take advantage of Azure marketplace direct deployment, a streamlined process that provides access to a limited, but still powerful set of Cloud Volumes ONTAP features and options.

When you deploy Cloud Volumes ONTAP directly from the Azure marketplace, you're not required to set up the Console agent or meet other security and onboarding criteria required for deploying Cloud Volumes ONTAP through the Console. From the Azure marketplace, you can quickly deploy Cloud Volumes ONTAP in a few clicks and explore its core features and capabilities in your environment.

On completing the deployment in the Azure marketplace, you can discover these systems in the Console. After discovery, you can manage them as Cloud Volumes ONTAP systems and take advantage of all the Console capabilities. Refer to Discover the deployed systems in the Console.

Here is the feature comparison between the two options. Note that the features of a standalone instance deployed through the Azure marketplace change when it is discovered in the Console.

	Azure marketplace	NetApp Console
Onboarding	Shorter and easier, minimal preparation required for direct deployment	Longer onboarding process, including the installation of the Console agent
Supported virtual machine (VM) types	Eds_v5 and Ls_v3 instance types	Full range of VM types. Supported configurations in Azure
License	Free license	Any capacity-based license. Cloud Volumes ONTAP licensing

	Azure marketplace	NetApp Console
NetApp support	Not included	Available, based on the license type
Capacity	Up to 500 GiB	Expandable by configuration
Deployment model	High-availability (HA) mode deployment in single availability zone (AZ)	All supported configurations, including single node and HA modes, single and multiple AZ deployments
Supported disk type	Premium SSD v2 Managed Disks	Wider support. Default configuration for Cloud Volumes ONTAP
Write speed (fast write mode)	Not supported	Supported, based on your configuration. Learn about write speeds in Cloud Volumes ONTAP.
Orchestration capabilities	Not available	Available through NetApp Console, based on the license type
Number of supported storage VMs	One per deployment	Multiple storage VMs, based on your configuration. Supported number of storage VMs
Changing the instance type	Not supported	Supported
FabricPool tiering	Not supported	Supported

Related links

- Azure marketplace direct deployment: Deploy Cloud Volumes ONTAP from the Azure marketplace
- Deployment through the Console: Quick start for Cloud Volumes ONTAP in Azure
- NetApp Console documentation

Get started in NetApp Console

Quick start for Cloud Volumes ONTAP in Azure

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

1

Create a Console agent

If you don't have a Console agent yet, you need to create one. Learn how to create a Console agent in Azure

Note that if you want to deploy Cloud Volumes ONTAP in a subnet where no internet access is available, then you need to manually install the Console agent and access the NetApp Console that's running on that Console agent. Learn how to manually install the Console agent in a location without internet access

2

Plan your configuration

The Console 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.

For information, refer to Plan your Cloud Volumes ONTAP configuration in Azure.

3 **Set up your networking**

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

b. Enable outbound internet access from the target VPC for NetApp AutoSupport.

   This step isn't required if you're deploying Cloud Volumes ONTAP in a location where no internet access is available.

Learn more about networking requirements.

4 **Launch Cloud Volumes ONTAP**

Click **Add System**, 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 Console agent from the Console
- Creating a Console agent from the Azure Marketplace
- Installing the Console agent software on a Linux host
- What the Console 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 with single-node systems

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

Single-node systems can use these types of Azure Managed Disks:

- *Premium SSD Managed Disks* provide high performance for I/O-intensive workloads at a higher cost.
- *Premium SSD v2 Managed Disks* provide higher performance with lower latency at a lower cost, compared to Premium SSD Managed Disks.
- *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, refer to Microsoft Azure Documentation: What disk types are available in Azure?.

Azure disk type with HA pairs

HA systems use Premium SSD Shared Managed Disks which both provide high performance for I/O-intensive workloads at a higher cost. HA deployments created before the 9.12.1 release use Premium page blobs.

Azure disk size

When you launch Cloud Volumes ONTAP instances, you must choose the default disk size for aggregates. The NetApp Console 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, the Console 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 Console agent also requires a system disk. View details about the Console agent'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	
Virtual network (VNet)	
Subnet	
Network security group (if using your own)	

Choose a write speed

The Console 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 the Console, 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.

Set up Azure networking for Cloud Volumes ONTAP

The NetApp Console handles the set up of networking components for Cloud Volumes ONTAP, such as IP addresses, netmasks, and routes. You need to make sure that outbound internet access is available, that enough private IP addresses are available, that the right connections are in place, and more.

Requirements for Cloud Volumes ONTAP

The following networking requirements must be met in Azure.

Outbound internet access

Cloud Volumes ONTAP systems require outbound internet access for accessing external endpoints for various functions. Cloud Volumes ONTAP can't operate properly if these endpoints are blocked in environments with strict security requirements.

The Console agent also contacts several endpoints for day-to-day operations. For information about endpoints, refer to View endpoints contacted from the Console agent and Prepare networking for using the Console.

Cloud Volumes ONTAP endpoints

Cloud Volumes ONTAP uses these endpoints to communicate with various services.

Endpoints	Applicable for	Purpose	Deployment modes	Impact if unavailable
https://netapp-cloud-account.auth0.com	Authentication	Used for authentication in the Console.	Standard and restricted modes.	User authentication fails and the following services remain unavailable: • Cloud Volumes ONTAP services • ONTAP services • Protocols and proxy services

Endpoints	Applicable for	Purpose	Deployment modes	Impact if unavailable
https://vault.azure.net	Key Vault	Used to retrieve client secret keys from the Azure Key Vault when using customer-managed keys (CMK).	Standard, restricted, and private modes.	Cloud Volumes ONTAP services are unavailable.
https://api.bluexp.netapp.com/tenancy	Tenancy	Used to retrieve the Cloud Volumes ONTAP resources from the Console to authorize resources and users.	Standard and restricted modes.	Cloud Volumes ONTAP resources and the users are not authorized.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Used to send AutoSupport telemetry data to NetApp support.	Standard and restricted modes.	AutoSupport information remains undelivered.
https://management.azure.com https://login.microsoftonline.com https://bluexpinfraprod.eastus2.data.azurecr.io https://core.windows.net	Public regions	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	China Region	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.
https://management.microsoftazure.de https://login.microsoftonline.de https://blob.core.cloudapi.de https://core.cloudapi.de	Germany Region	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Government regions	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.

Endpoints	Applicable for	Purpose	Deployment modes	Impact if unavailable
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Government DoD regions	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.

Network proxy configuration of NetApp Console agent

You can use the proxy servers configuration of the NetApp Console agent to enable outbound internet access from Cloud Volumes ONTAP. The Console supports two types of proxies:

- **Explicit proxy**: The outbound traffic from Cloud Volumes ONTAP uses the HTTP address of the proxy server specified during the proxy configuration of the Console agent. The administrator might also have configured user credentials and root CA certificates for additional authentication. If a root CA certificate is available for the explicit proxy, make sure to obtain and upload the same certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.
- **Transparent proxy**: The network is configured to automatically route outbound traffic from Cloud Volumes ONTAP through the proxy for the Console agent. When setting up a transparent proxy, the administrator needs to provide only a root CA certificate for connectivity from Cloud Volumes ONTAP, not the HTTP address of the proxy server. Make sure that you obtain and upload the same root CA certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.

For information about configuring proxy servers, refer to the Configure the Console agent to use a proxy server.

IP addresses

The Console automatically allocates the required number of private IP addresses to Cloud Volumes ONTAP in Azure. You need to make sure that your networking has enough private IP addresses available.

The number of LIFs allocated for Cloud Volumes ONTAP depends on whether you deploy a single-node system or an HA pair. A LIF is an IP address associated with a physical port. An SVM management LIF is required for management tools like SnapCenter.

> An iSCSI LIF provides client access over the iSCSI protocol and is used by the system for other important networking workflows. These LIFs are required and should not be deleted.

IP addresses for a single-node system

The Console allocates 5 or 6 IP addresses to a single-node system:

- Cluster management IP
- Node management IP
- Intercluster IP for SnapMirror
- NFS/CIFS IP

- iSCSI IP

> The iSCSI IP provides client access over the iSCSI protocol. It is also used by the system for other important networking workflows. This LIF is required and should not be deleted.

- SVM management (optional - not configured by default)

IP addresses for HA pairs

The Console allocates IP addresses to 4 NICs (per node) during deployment.

Note that the Console creates an SVM management LIF on HA pairs, but not on single-node systems in Azure.

NIC0

- Node management IP
- Intercluster IP
- iSCSI IP

> The iSCSI IP provides client access over the iSCSI protocol. It is also used by the system for other important networking workflows. This LIF is required and should not be deleted.

NIC1

- Cluster network IP

NIC2

- Cluster Interconnect IP (HA IC)

NIC3

- Pageblob NIC IP (disk access)

> NIC3 is only applicable to HA deployments that use page blob storage.

The above IP addresses do not migrate on failover events.

Additionally, 4 frontend IPs (FIPs) are configured to migrate on failover events. These frontend IPs live in the load balancer.

- Cluster management IP
- NodeA data IP (NFS/CIFS)
- NodeB data IP (NFS/CIFS)
- SVM management IP

Secure connections to Azure services

By default, the Console enables an Azure Private Link for connections between Cloud Volumes ONTAP and Azure page blob storage accounts.

In most cases, there's nothing that you need to do—the Console 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 location of the Console agent in Azure.

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

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

Networking for Azure VNet encryption

Cloud Volumes ONTAP supports Azure Virtual Network (VNet) encryption for encrypting VM-to-VM traffic inside a VNet or across peered VNets. This feature is configured at the Azure VNet layer and is independent of Cloud Volumes ONTAP topology (single node or HA).

You only need to ensure that Accelerated Networking is enabled on the VM's NICs and review Azure VNet encryption requirements and limitations before enabling the feature. You should not modify NetApp managed load balancer objects.

Azure documentation: VNet encryption and Accelerated Networking.

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 the 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.

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

Security group rules

The Console creates Azure security groups that include the inbound and outbound rules for Cloud Volumes ONTAP to operate successfully. View security group rules for the Console agent.

The Azure security groups for Cloud Volumes ONTAP require the appropriate ports to be open for internal communication between the nodes. Learn about ONTAP internal ports.

We do not recommend modifying the predefined security groups or using custom security groups. However, if you must, note that the deployment process requires the Cloud Volumes ONTAP system to have full access within its own subnet. After the deployment is complete, if you decide to modify the network security group, ensure to keep the cluster ports and HA network ports open. This ensures seamless communication within the Cloud Volumes ONTAP cluster (any-to-any communication between the nodes).

Inbound rules for single-node systems

When you add a Cloud Volumes ONTAP system 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 Console agent resides. This is the recommended option.
- **All VNets**: The source for inbound traffic is the 0.0.0.0/0 IP range.
- **Disabled**: This option restricts the public network access to your storage account, and disables data tiering for Cloud Volumes ONTAP systems. This is a recommended option if your private IP addresses should not be exposed even within the same VNet due to security regulations and policies.

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 ONTAP 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
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 Console agent and HTTPS access to the ONTAP 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

Priority and name	Port and protocol	Source and destination	Description
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
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 AllowAzureLoadBalancerInBound	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 add a Cloud Volumes ONTAP system 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 Console agent resides. This is the recommended option.
- **All VNets**: The source for inbound traffic is the 0.0.0.0/0 IP range.

> 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.

- **Disabled**: This option restricts the public network access to your storage account, and disables data tiering for Cloud Volumes ONTAP systems. This is a recommended option if your private IP addresses should not be exposed even within the same VNet due to security regulations and policies.

Priority and name	Port and protocol	Source and destination	Description
100 inbound_443	443 Any protocol	Any to Any	Connectivity with the Console agent and HTTPS access to the ONTAP 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
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	mysupport.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	mysupport.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Console agent	Sending AutoSupport messages through a proxy server on the Console agent, if an outbound internet connection isn't available
Configuration backups	HTTP	80	Node management LIF	http://<console-agent-IP-address>/occm/offboxconfig	Send configuration backups to the Console agent. ONTAP documentation.
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 Console agent

If you haven't created a Console agent yet, you should review networking requirements for the Console agent as well.

- View networking requirements for the Console agent
- Security group rules in Azure

Related topics

- Verify AutoSupport setup for Cloud Volumes ONTAP
- Learn about ONTAP internal ports.

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 the NetApp Console, use the API to create a Cloud Volumes ONTAP system that uses the key.

How data is encrypted

The Console uses a disk encryption set, which enables management of encryption keys with managed disks not page blobs. Any new data disks also use the same disk encryption set. Lower versions will use Microsoft-managed key, instead of the customer-managed key.

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

Cloud Volumes ONTAP configuration	System disks used for key encryption	Data disks used for key encryption
Single node	• Boot • Core • NVRAM	• Root • Data
Azure HA single availability zone with page blobs	• Boot • Core • NVRAM	None

Cloud Volumes ONTAP configuration	System disks used for key encryption	Data disks used for key encryption
Azure HA single availability zone with shared managed disks	• Boot • Core • NVRAM	• Root • Data
Azure HA multiple availability zones with shared managed disks	• Boot • Core • NVRAM	• Root • Data

All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key. If you want to encrypt your storage accounts during their creation, you must create and provide the ID of the resource in the Cloud Volumes ONTAP creation request. This applies for all type of deployments. If you do not provide it, the storage accounts still will be encrypted, but the Console first creates the storage accounts with Microsoft-managed key encryption and then updates the storage accounts to use the customer-managed key.

Key rotation in Cloud Volumes ONTAP

When you configure your encryption keys, you must use the Azure portal to set up and enable automatic key rotation. Creating and enabling a new version of encryption keys ensures that Cloud Volumes ONTAP can automatically detect and use the latest key version for encryption, ensuring your data remains secure without the need for manual intervention.

For information about configuring your keys and setting up key rotation, refer to the following Microsoft Azure documentation topics:

- Configure cryptographic key auto-rotation in Azure Key Vault
- Azure PowerShell - Enable customer-managed keys

> ⓘ After configuring the keys, ensure that you have selected *Enable auto rotation*, so that Cloud Volumes ONTAP can use the new keys when the previous keys expire. If you don't enable this option on the Azure portal, Cloud Volumes ONTAP can't automatically detect the new keys, which might cause issues with storage provisioning.

Create a user-assigned managed identity

You have the option to create a resource called a user-assigned managed identity. Doing so allows you to encrypt your storage accounts when you create a Cloud Volumes ONTAP system. We recommend creating this resource prior to creating a key vault and generating a key.

The resource has the following ID: `userassignedidentity`.

Steps

1. In Azure, go to Azure services and select **Managed Identities**.
2. Click **Create**.
3. Provide the following details:
   - **Subscription**: Choose a subscription. We recommend choosing the same subscription as the subscription of the Console agent.

◦ **Resource group**: Use an existing resource group or create a new one.
◦ **Region**: Optionally, select the same region as the Console agent.
◦ **Name**: Enter a name for the resource.

4. Optionally, add tags.
5. Click **Create**.

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.

If you created a user-assigned managed identity, while creating the key vault, you should also create an access policy for the key vault.

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 systems, HA pairs in multiple zones, and HA single AZ deployments)

       > Usage of Azure customer-managed encryption keys is contingent upon having Azure Disk encryption enabled for the key vault.

   ◦ The following option should be enabled if you created a user-assigned managed identity:
     ▪ **Vault access policy**

2. If you selected Vault access policy, click Create to create an access policy for the key vault. If not, skip to step 3.

   a. Select the following permissions:
      ▪ get
      ▪ list
      ▪ decrypt
      ▪ encrypt
      ▪ unwrap key
      ▪ wrap key
      ▪ verify
      ▪ sign

   b. Select the user-assigned managed identity (resource) as the principal.
   c. Review and create the access policy.

3. 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 system 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 API.

Required permissions

If you want to use a customer-managed key with a single node Cloud Volumes ONTAP system, ensure that the Console agent 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",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

View the latest list of permissions

Steps

1. Obtain the list of key vaults in your Azure subscription by using the following 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 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 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"
}
```

Include the `"userAssignedIdentity": " userAssignedIdentityId"` field if you created this resource to be used for storage account encryption.

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"
}
```

Include the `"userAssignedIdentity": " userAssignedIdentityId"` field if you created this resource to be used for storage account encryption.

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 system.

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.

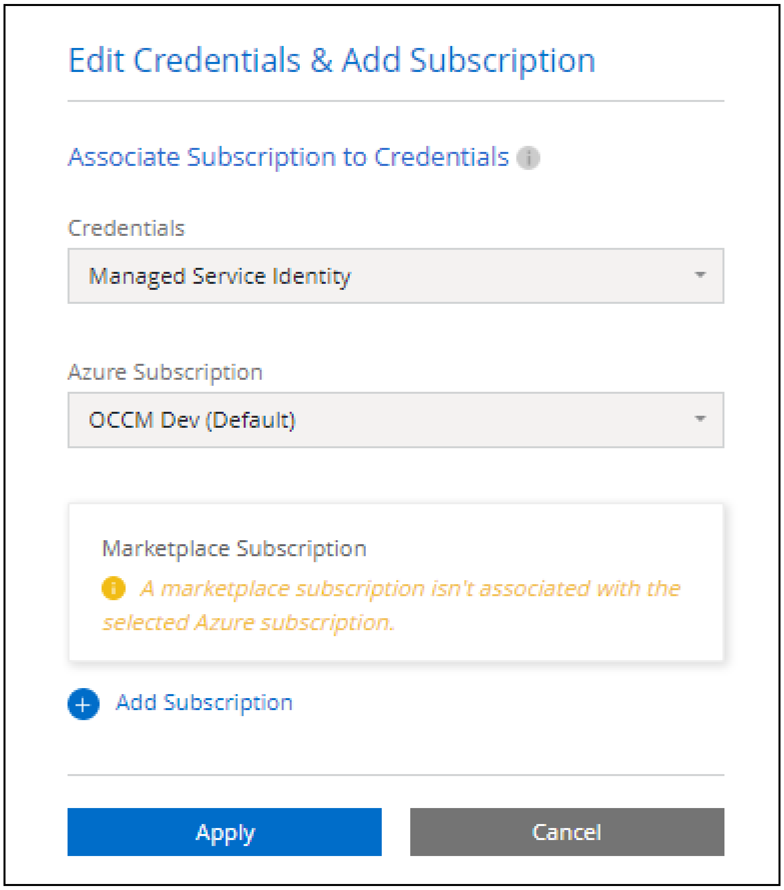
Steps

1. From the left navigation menu of the NetApp Console, select **Storage > Management**.

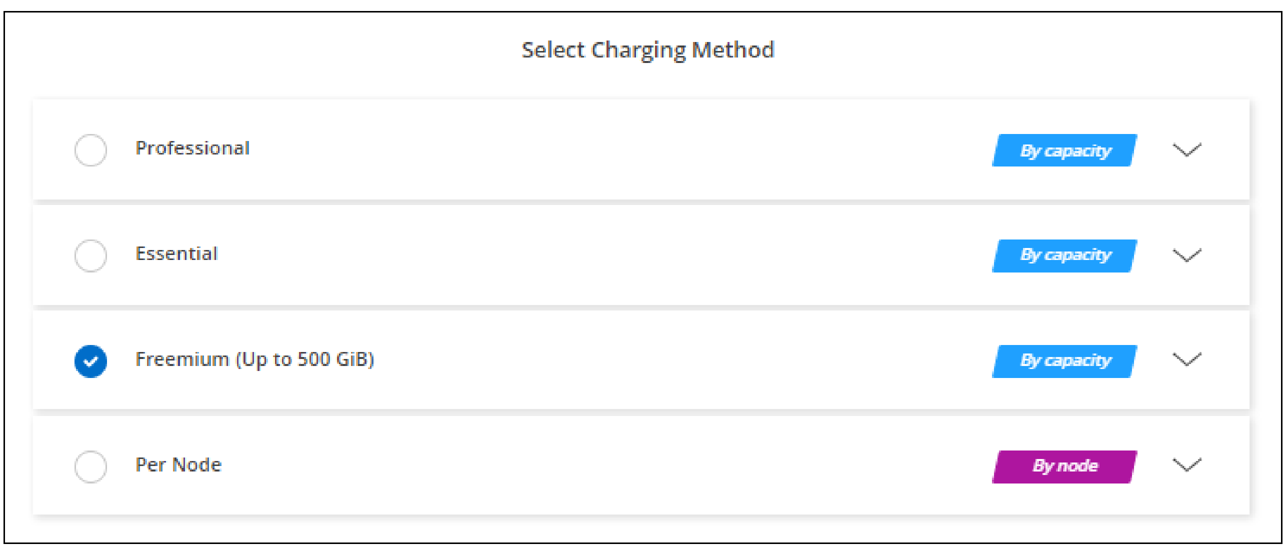
2. On the **Systems** page, click **Add System** and follow the steps.

   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 the Console, 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 or purchase options:

- A license (bring your own 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.

> NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP.

Steps

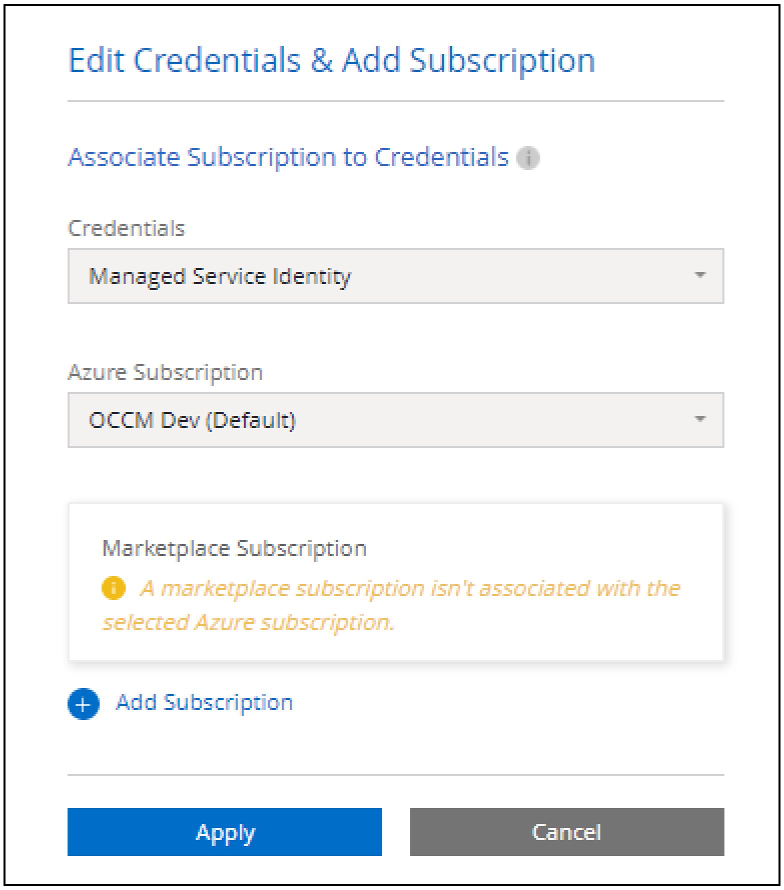
1. Contact NetApp Sales to obtain a license
2. Add your NetApp Support Site account to the Console

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

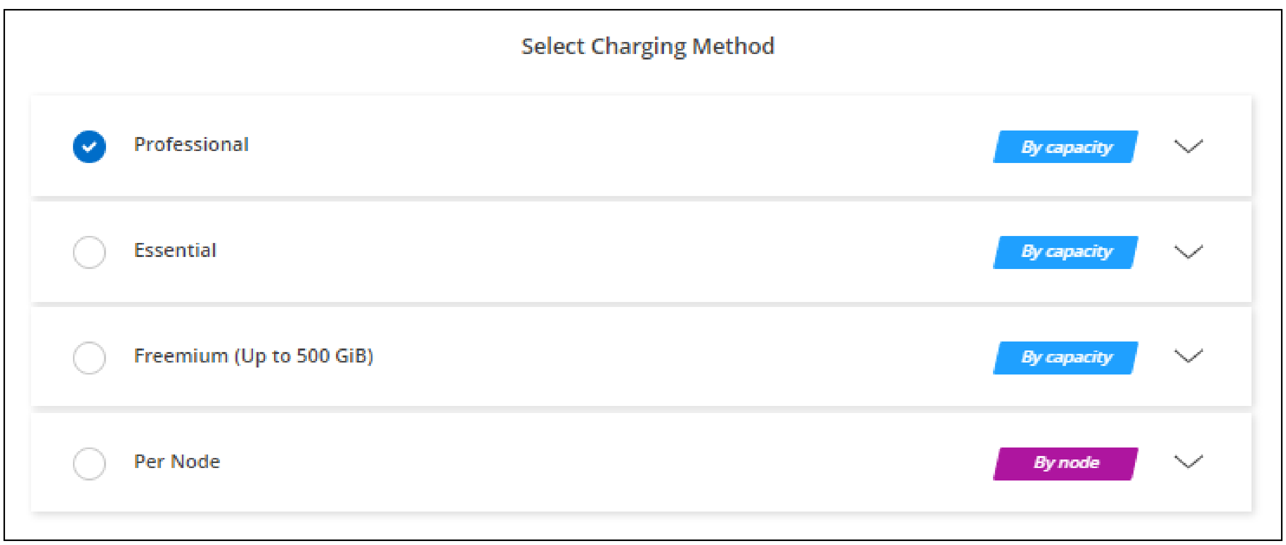
   Your license must be available from the Console before you can use it with Cloud Volumes ONTAP. If needed, you can manually add the license to the Console.

3. On the **Systems** page, click **Add System** and follow the steps.
   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 the Console, 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

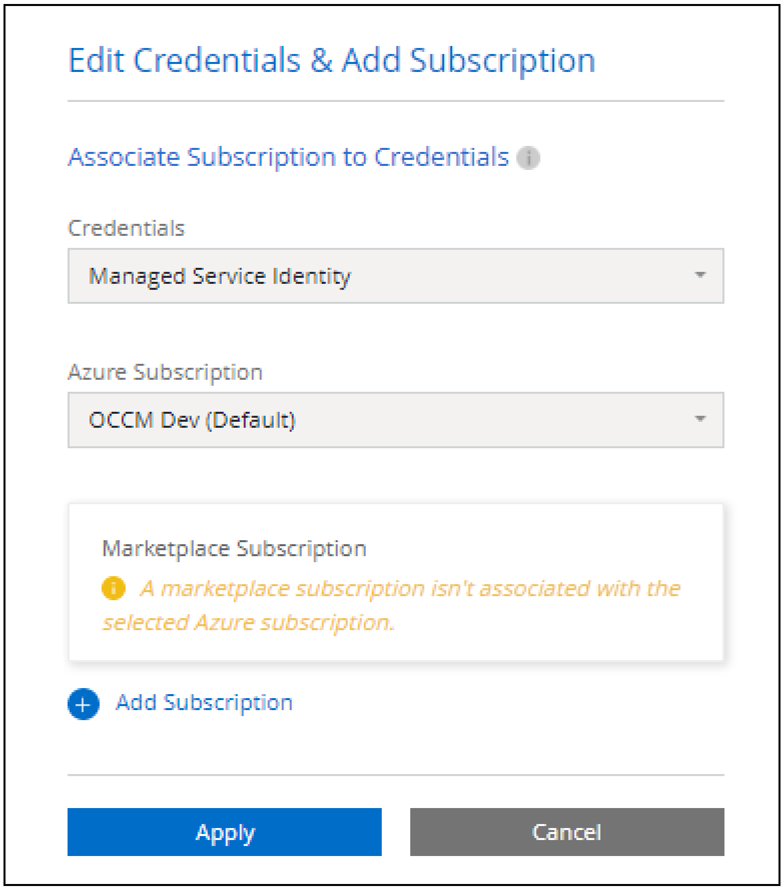
Pay hourly by subscribing to the offer from your cloud provider's marketplace.

When you create a Cloud Volumes ONTAP system, the Console prompts you to subscribe to the agreement that's available in the Azure Marketplace. That subscription is then associated with the system for charging.

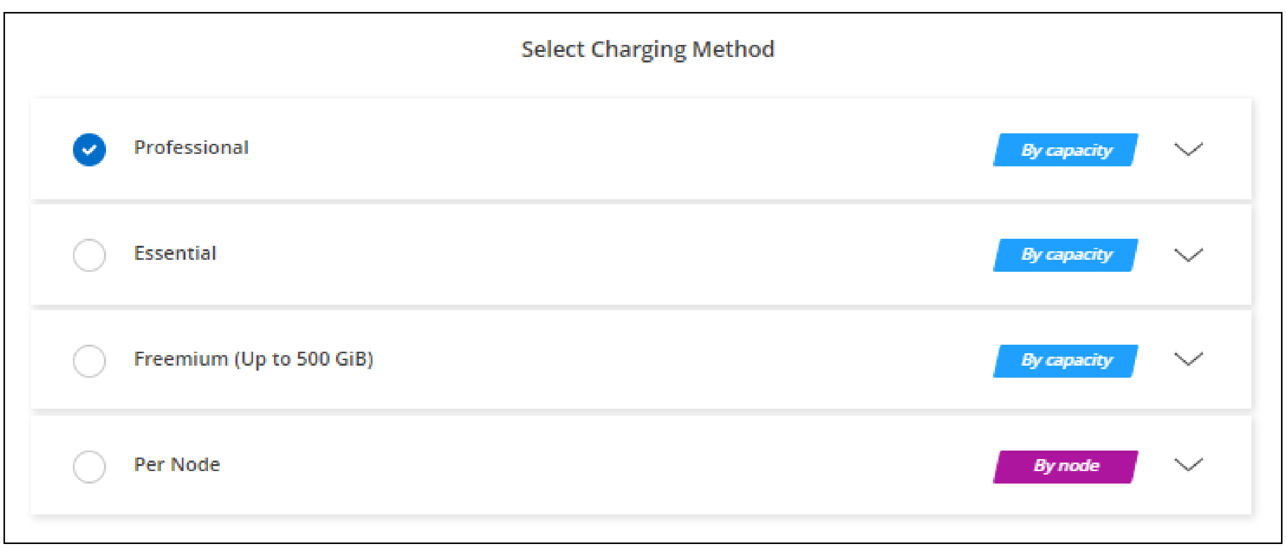
You can use that same subscription for additional systems.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the steps.
   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 the Console, 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.

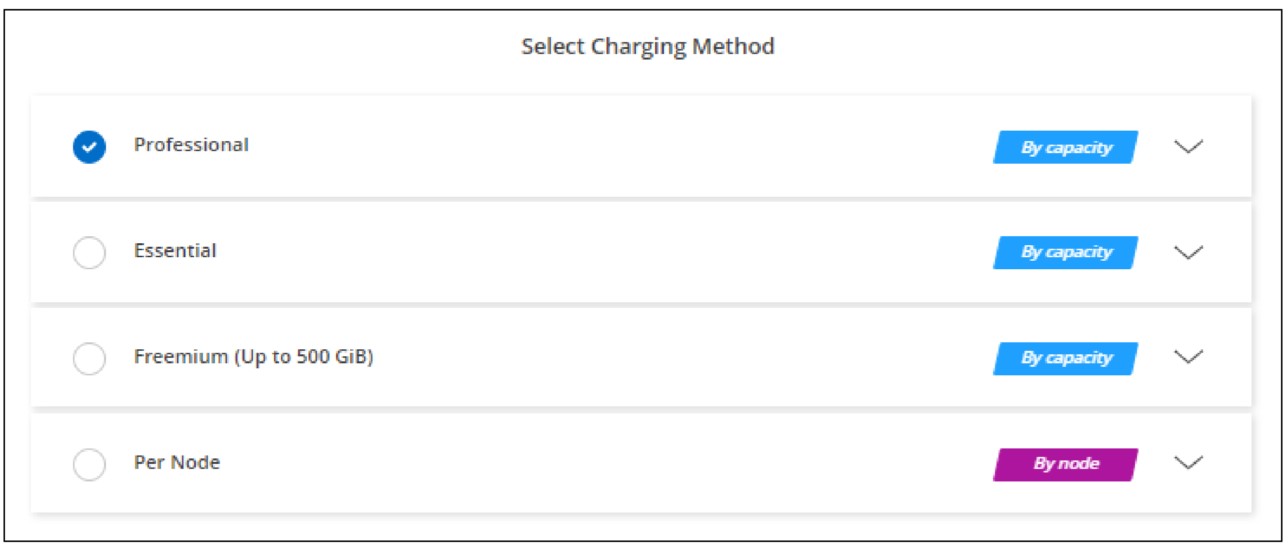
   After NetApp shares the private offer with you, you can select the annual plan when you subscribe from the Azure Marketplace during system creation.

2. On the **Systems** page, click **Add System** and follow the steps.

   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 the Console, select a capacity-based package when you reach the charging methods page.



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

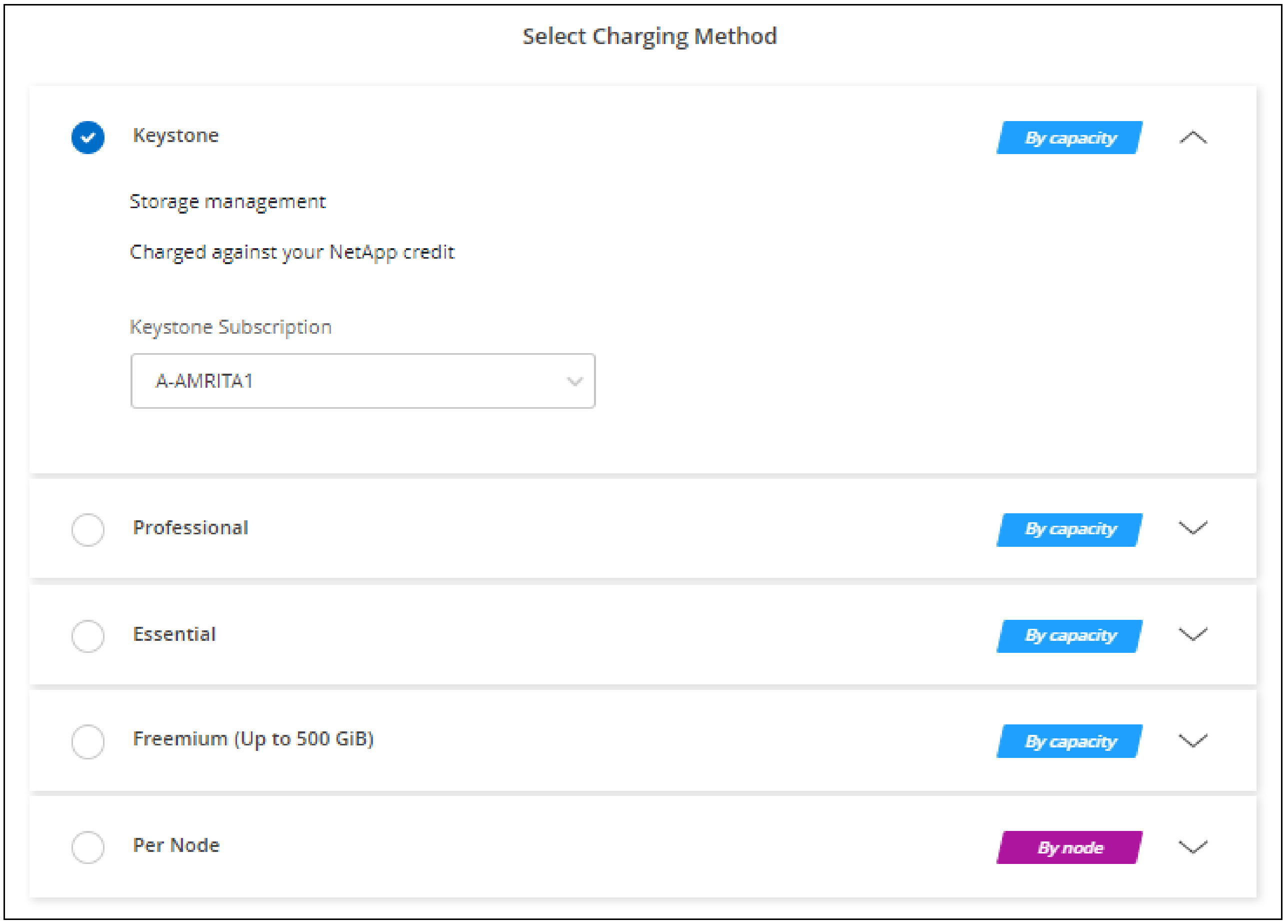
Keystone Subscription

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

Steps

1. If you don’t have a subscription yet, contact NetApp
2. Contact NetApp to authorize your user account in the Console with one or more Keystone Subscriptions.

3. After NetApp authorizes your account, link your subscriptions for use with Cloud Volumes ONTAP.
4. On the **Systems** page, click **Add System** and follow the steps.
   a. Select the Keystone Subscription charging method when prompted to choose a charging method.



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

Node-based license

A node-based license is the previous generation license for Cloud Volumes ONTAP. A node-based license could be procured from NetApp (BYOL) and is available for license renewals, only in specific cases. For information, refer to:

- End of availability for node-based licenses
- End of availability of node-based licenses
- Convert a node-based license to a capacity-based license

Enable high-availability mode for Cloud Volumes ONTAP in Azure

You should enable Microsoft Azure's high-availability (HA) mode to reduce unplanned failover times and to enable NFSv4 support for Cloud Volumes ONTAP. If you enable this mode, your Cloud Volumes ONTAP HA nodes can achieve a low (60 seconds) recovery time objective (RTO) during unplanned failovers on CIFS and NFSv4 clients.

Beginning with Cloud Volumes ONTAP 9.10.1, 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.

About this task

NetApp Console prompts you with these details 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 doesn't cause issues to other VMs.
- Cloud Volumes ONTAP uses an internal Azure Load Balancer during failovers of cluster and SVM management LIFs on CIFS and NFS clients.
- When the HA mode is enabled, the Console scans the system every 12 hours to update the internal Azure Load Balancer rules.

Steps

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

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"
}
```


Related links

1. Microsoft Azure documentation: High availability ports overview
2. Microsoft Azure documentation: Get started with Azure CLI

Enable VMOrchestratorZonalMultiFD for Cloud Volumes ONTAP in Azure

For deploying VM instances in locally-redundant storage (LRS) single availability zones (AZ), you should activate the Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` feature for your subscriptions. In a high-availability (HA) mode, this feature facilitates deploying nodes in separate fault domains in the same availability zone.

Unless you activate this feature, zonal deployment doesn't occur, and the previous LRS non-zonal deployment becomes effective.

For information about VM deployment in single availability zone, refer to High-availability pairs in Azure.

Perform these steps as a user with "Owner" privileges:

Steps

1. Access Azure Cloud Shell from the Azure portal. For information, refer to the Microsoft Azure documentation: Get started with Azure Cloud Shell.
2. Register for the `Microsoft.Compute/VMOrchestratorZonalMultiFD` feature by running this command:

```
az account set -s <Azure_subscription_name_or_ID>
az feature register --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
```

3. Verify the registration status and output sample:

```
az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
{
"id": "/subscriptions/
<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiF
D",
"name": "Microsoft.Compute/VMOrchestratorZonalMultiFD",
"properties": {
"state": "Registered"
},
"type": "Microsoft.Features/providers/features"
}
```

Launch Cloud Volumes ONTAP in Azure

You can launch a single-node system or an HA pair in Azure by creating a Cloud Volumes ONTAP system in NetApp Console.

Before you begin

You need the following before you begin.

- A Console agent that's up and running.
  - You should have a Console agent that is associated with your system.
  - You should be prepared to leave the Console agent running at all times.
- An understanding of the configuration that you want to use.

  You should have a configuration planned, and the necessary Azure networking details from your administrator. For more information, refer to 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 the Console 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 the Console 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.

Launch a single-node Cloud Volumes ONTAP system in Azure

If you want to launch a single-node Cloud Volumes ONTAP system in Azure, you need to create an single-node system in the Console.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the prompts.
3. **Choose a Location**: Select **Microsoft Azure** and **Cloud Volumes ONTAP Single Node**.
4. If you're prompted, create a Console agent.
5. **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
System Name	The Console uses the system 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, the Console 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 system, and then you can add more after it's created. Note that the API does not limit you to four tags when creating a system. For information about tags, refer to the Microsoft Azure Documentation: Using tags to organize your Azure resources.
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 ONTAP System Manager or the ONTAP 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.

6. **Services**: Enable or disable the individual services that you want to or don't want to use with Cloud Volumes ONTAP.
   - Learn more about NetApp Data Classification
   - Learn more about NetApp Backup and Recovery

   > If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

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

For China regions, single node deployments are supported only in Cloud Volumes ONTAP 9.12.1 GA and 9.13.0 GA. You can upgrade these versions to later patches and releases of Cloud Volumes ONTAP as supported in Azure. If you want to deploy later Cloud Volumes ONTAP versions in China regions, contact NetApp Support. Only licenses purchased directly from NetApp are supported in China regions, marketplace subscriptions are not available.

8. **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
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. If the Azure account that you're using has the required permissions, the Console removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.
Generated security group	If you let the Console 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 Console agent 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.

9. **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.
10. **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.
11. **Licensing**: Change the Cloud Volumes ONTAP version if required, and select a virtual machine type.

> If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.16.1 P3 and 9.16.1 P4 is available. The update does not occur from one release to another—for example, from 9.15 to 9.16.

12. **Subscribe from the Azure Marketplace**: You see this page if the Console could not enable programmatic deployments of Cloud Volumes ONTAP. Follow the steps listed on the screen. refer to Programmatic deployment of Marketplace products for more information.
13. **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:

    - If the public access to your storage account is disabled within the VNet, you cannot enable data tiering in your Cloud Volumes ONTAP system. For information, refer to Security group rules.
    - 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 the Console 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, refer to 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.
14. **Write Speed & WORM**:
    a. Choose **Normal** or **High** write speed, if desired.

       Learn more about write speed.

    b. Activate write once, read many (WORM) storage, if desired.

       This option is only available for certain VM types. To find out which VM types are supported, refer to Supported configurations by license for HA pairs.

       WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

       Learn more about WORM storage.

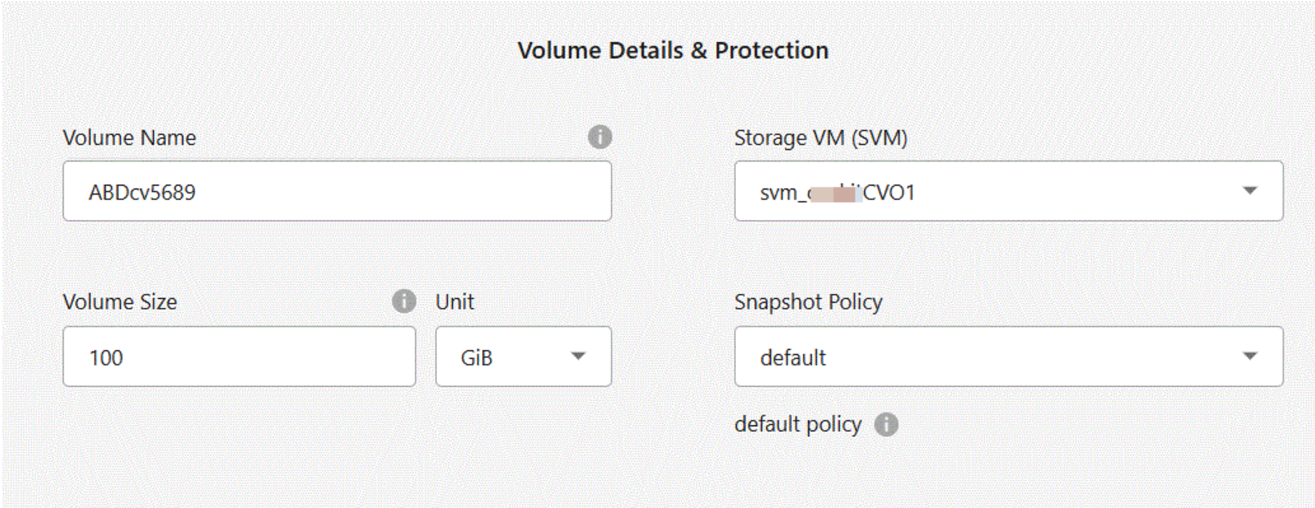
    c. If you activate WORM storage, select the retention period.
15. **Create Volume**: Enter details for the new volume or click **Skip**.

    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, the Console 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, the Console 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 first page of the volume creation wizard:



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. Refer to the NetApp Console 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, refer to 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 the Console will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

Result

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the Audit page.

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

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

> After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Azure portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

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 ONTAP System Manager or the ONTAP CLI.

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

Launch a Cloud Volumes ONTAP HA pair in Azure

If you want to launch a Cloud Volumes ONTAP HA pair in Azure, you need to create an HA system in the Console.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the prompts.
3. If you're prompted, create a Console agent.
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
System Name	The Console uses the system 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.

Field	Description
Resource Group Tags	Tags are metadata for your Azure resources. When you enter tags in this field, the Console 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 system, and then you can add more after it's created. Note that the API does not limit you to four tags when creating a system. For information about tags, refer to the Microsoft Azure Documentation: Using tags to organize your Azure resources.
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 ONTAP System Manager or the ONTAP 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.

5. **Services**: Enable or disable the individual services based on whether you want to use them with Cloud Volumes ONTAP.
   - Learn more about NetApp Data Classification
   - Learn more about NetApp Backup and Recovery

   If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

6. **HA Deployment Models**:
   a. Select **Single Availability Zone** or **Multiple Availability Zone**.
      - For single availability zones, select an Azure region, availability zone, VNet, and subnet.

        Beginning with Cloud Volumes ONTAP 9.15.1, you can deploy virtual machine (VM) instances in HA mode in single availability zones (AZs) in Azure. You need to select a zone and a region that support this deployment. If the zone or the region does not support zonal deployment, then the previous non-zonal deployment mode for LRS is followed. For understanding the supported configurations for shared managed disks, refer to HA single availability zone configuration with shared managed disks.
      - For multiple availability zones, select a region, VNet, subnet, zone for node 1, and zone for node 2.

   b. Select the **I have verified network connectivity…** check box.
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
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. The Console 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, the Console removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.
Generated security group	If you let the Console 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 Console agent 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 **Change 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 the Console updates the system to that version when creating it. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another— for example, from 9.13 to 9.14.
11. **Subscribe from the Azure Marketplace**: Follow the steps if the Console 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 size is for all disks in the initial aggregate and for any additional aggregates that the Console 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 size, refer to Size your system in Azure.

    - If the public access to your storage account is disabled within the VNet, you cannot enable data tiering in your Cloud Volumes ONTAP system. For information, refer to Security group rules.
    - 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.

    - Starting with Cloud Volumes ONTAP 9.15.0P1, Azure page blobs are no longer supported for new high-availability pair deployments. If you currently use Azure page blobs in existing high-availability pair deployments, you can migrate to newer VM instance types in the Edsv4-series VMs and Edsv5-series VMs.

      Learn more about supported configurations in Azure.

13. **Write Speed & WORM**:
    a. Choose **Normal** or **High** write speed, if desired.

       Learn more about write speed.

    b. Activate write once, read many (WORM) storage, if desired.

       This option is only available for certain VM types. To find out which VM types are supported, refer to Supported configurations by license for HA pairs.

       WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

       Learn more about WORM storage.

    c. If you activate WORM storage, select the retention period.
14. **Secure Communication to Storage & WORM**: 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 page blob storage accounts. Note that enabling this option can impact write performance. You can't change the setting after you create the system.

    Learn more about WORM storage.

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

    Learn more about WORM storage.

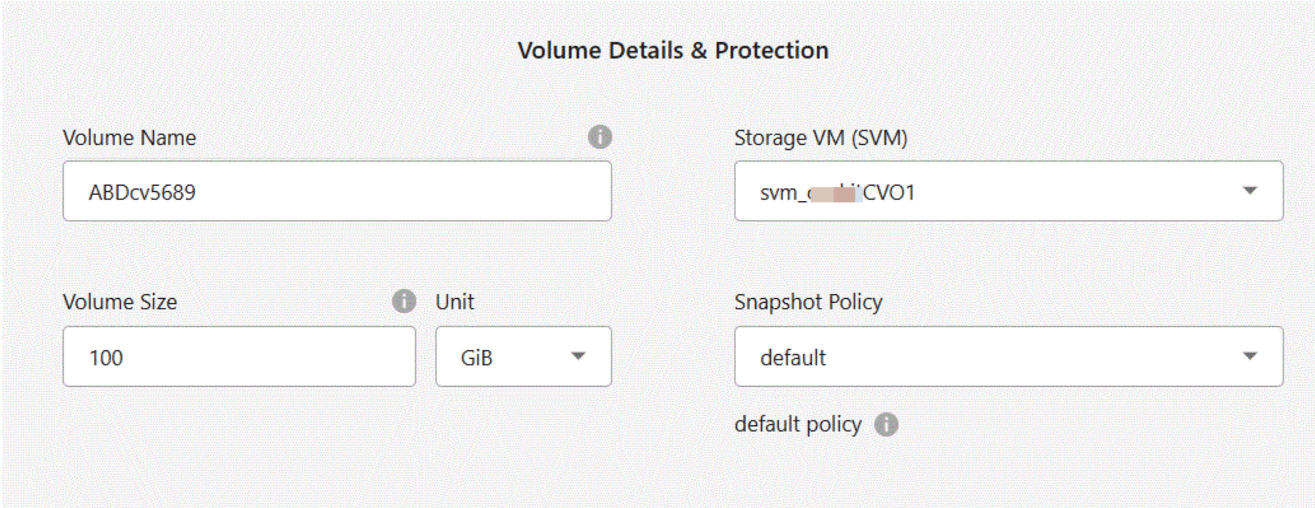
15. **Create Volume**: Enter details for the new volume or click **Skip**.

    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, the Console 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, the Console 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 first page of the volume creation wizard:



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. Refer to the NetApp Console 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, refer to Choose a volume usage profile, Data tiering overview, and KB: What Inline Storage Efficiency features are supported with CVO?

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 the Console will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

Result

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the Audit page.

If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the system 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 ONTAP System Manager or the ONTAP CLI.

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

> After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Azure portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

Related links

*Planning your Cloud Volumes ONTAP configuration in Azure
*Deploy Cloud Volumes ONTAP in Azure from the Azure Marketplace

Verify Azure platform image

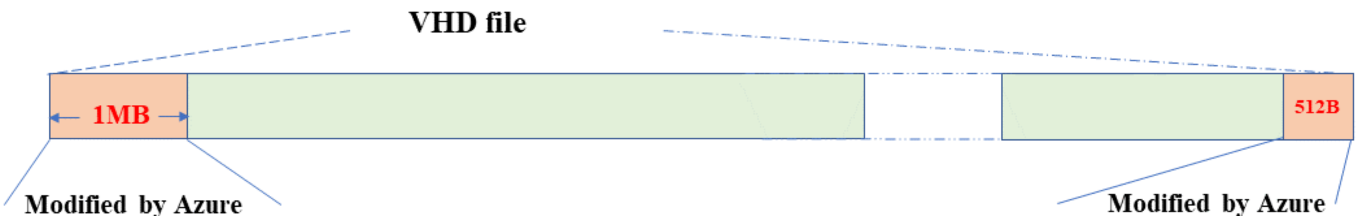
Azure marketplace image verification for Cloud Volumes ONTAP

Azure image verification complies with enhanced NetApp security requirements. Verifying an image file is a straightforward process. However, the Azure image signature verification requires specific considerations for the Azure VHD image file because it is altered in the Azure marketplace.

> Azure image verification is supported on Cloud Volumes ONTAP 9.15.0 and later.

Azure's alteration of published VHD files

The 1 MB (1048576 bytes) at the beginning and 512 bytes at the end of the VHD file is modified by Azure. NetApp signs the remaining VHD file.



In the example, the VHD file is of 10GB. The portion that NetApp signed is marked in green (10 GB - 1 MB - 512 bytes).

Related links

- Page Fault Blog: How to sign and verify using OpenSSL
- Use Azure Marketplace image to create VM image for your Azure Stack Edge Pro GPU | Microsoft Learn
- Export/Copy a managed disk to a storage account using the Azure CLI | Microsoft Learn
- Azure Cloud Shell Quickstart - Bash | Microsoft Learn
- How to install the Azure CLI | Microsoft Learn
- az storage blob copy | Microsoft Learn
- Sign in with Azure CLI — Login and Authentication | Microsoft Learn

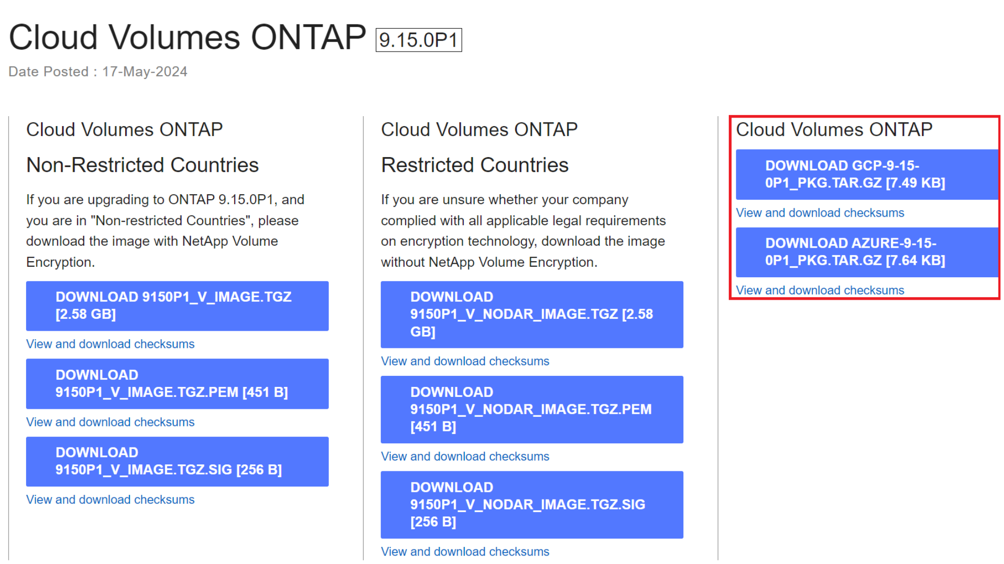
Download the Azure image file for Cloud Volumes ONTAP

You can download the Azure image file from the NetApp Support Site.

The *tar.gz* file contains the files required for image signature verification. Along with the *tar.gz* file, you should also download the *checksum* file for the image. The checksum file contains the `md5` and `sha256` checksums of the *tar.gz* file.

Steps

1. Go to the Cloud Volumes ONTAP product page on the NetApp Support Site and download the required software version from the **Downloads** section.
2. On the Cloud Volumes ONTAP download page, click the downloadable file for the Azure image and download the *tar.gz* file.



3. On Linux, run `md5sum AZURE-<version>_PKG.TAR.GZ`.

   On macOS, run `sha256sum AZURE-<version>_PKG.TAR.GZ`.

4. Verify that the `md5sum` and `sha256sum` values match those in the downloaded Azure image.
5. On Linux and macOS, extract the *tar.gz* file using the `tar -xzf` command.

   The extracted *tar.gz* file contains the digest (*.sig*) file, public key certificate (*.pem*) file, and chain certificate (*.pem*) file.

   Example output after extracting the tar.gz file:

   ```
   $ ls cert/ -l
   -rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
   -rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
   9.15.0P1_azure.pem
   -rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
   9.15.0P1_azure.pem
   -rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
   ```

Export VHD images for Cloud Volumes ONTAP from the Azure marketplace

Once the VHD image is published to Azure cloud, it is no longer managed by NetApp. Instead, the published image is placed on the Azure marketplace. When the image is staged and published on the Azure marketplace, Azure modifies 1 MB at the beginning and 512 bytes at the end of the VHD. To verify the signature of the VHD file, you need to export the VHD image modified by Azure from the Azure marketplace.

Before you begin

Ensure that the Azure CLI is installed on your system, or the Azure Cloud Shell is available through the Azure portal. For more information about how to install the Azure CLI, refer to the [Microsoft documentation: How to install the Azure CLI].

Steps

1. Map the Cloud Volumes ONTAP version on your system to the Azure marketplace image version using the contents of the *version_readme* file. The Cloud Volumes ONTAP version is represented by `buildname` and the Azure marketplace image version is represented by `version` in the version mappings.

   In the following example, the Cloud Volumes ONTAP version `9.15.0P1` is mapped to the Azure marketplace image version `9150.01000024.05090105`. This Azure marketplace image version is later used to set the image URN.

```
[
 "buildname": "9.15.0P1",
    "publisher": "netapp",
     "version": "9150.01000024.05090105"

]
```

2. Identify the region where you want to create the VMs. The region name is used as the value for the `locName` variable when setting the URN of the marketplace image. To list the available regions, run this command:

```
az account list-locations -o table
```

In this table, the region name appears in the `Name` field.

```
$ az account list-locations -o table
DisplayName                Name                 RegionalDisplayName
------------------------   -------------------
------------------------------------
East US                    eastus               (US) East US
East US 2                  eastus2              (US) East US 2
South Central US           southcentralus       (US) South Central US
...
```

3. Review the SKU names for the corresponding Cloud Volumes ONTAP versions and VM deployment types in the table below. The SKU name is used as the value for the `skuName` variable when setting the URN of the marketplace image.

For example, all single node deployments with Cloud Volumes ONTAP 9.15.0 should use `ontap_cloud_byol` as the SKU name.

Cloud Volumes ONTAP version	VM deployment through	SKU name
9.17.1 and later	The Azure marketplace	ontap_cloud_direct_gen2
9.17.1 and later	The NetApp Console	ontap_cloud_gen2
9.16.1	The Azure marketplace	ontap_cloud_direct
9.16.1	The Console	ontap_cloud
9.15.1	The Console	ontap_cloud
9.15.0	The Console, single node deployments	ontap_cloud_byol
9.15.0	The Console, high availability (HA) deployments	ontap_cloud_byol_ha

4. After mapping the ONTAP version and Azure marketplace image, export the VHD file from the Azure marketplace using the Azure Cloud Shell or Azure CLI.

Export VHD file using the Azure Cloud Shell on Linux

From the Azure Cloud Shell, export the marketplace image to the VHD file (for example, *9150.01000024.05090105.vhd*), and download it to your local Linux system. Perform these steps to get the VHD image from the Azure marketplace.

Steps

1. Set the URN and other parameters of the marketplace image. The URN format is `<publisher>:<offer>:<sku>:<version>`. Optionally, you can list NetApp marketplace images to confirm the correct image version.

   ```
   PS /home/user1> $urn="netapp:netapp-ontap-
   cloud:ontap_cloud_byol:9150.01000024.05090105"
   PS /home/user1> $locName="eastus2"
   PS /home/user1> $pubName="netapp"
   PS /home/user1> $offerName="netapp-ontap-cloud"
   PS /home/user1> $skuName="ontap_cloud_byol"
   PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
   -Offer $offerName -Sku $skuName |select version
   ...
   141.20231128
   9.141.20240131
   9.150.20240213
   9150.01000024.05090105
   ...
   ```

2. Create a new managed disk from the marketplace image with the matching image version:

   ```
   PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
   PS /home/user1> $diskRG = “fnf1”
   PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
   $urn
   PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
   --access-level Read --name $diskName --resource-group $diskRG
   PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
   ```

3. Export the VHD file from the managed disk to Azure Storage. Create a container with the appropriate access level. In this example, we’ve used a container named `vm-images` with `Container` access level. Get the storage account access key from the Azure portal: **Storage Accounts > *examplesaname* > Access Key > *key1* > *key* > Show > *<copy>***

```
PS /home/user1> $storageAccountName = "examplesaname"
PS /home/user1> $containerName = "vm-images"
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = "9150.01000024.05090105.vhd"
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. Download the generated image to your Linux system. Use the `wget` command to download the VHD file:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

The URL follows a standard format. For automation, you can derive the URL string as shown below. Alternatively, you can use the Azure CLI `az` command to get the URL.
Example URL:
https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd

5. Clean up the managed disk

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Export VHD file using the Azure CLI on Linux

Export the marketplace image to a VHD file using the Azure CLI from a local Linux system.

Steps

1. Log in to the Azure CLI and list marketplace images:

```
% az login --use-device-code
```

2. To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the authentication code.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. Create a new managed disk from the marketplace image with the matching image version.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

To automate the process, the SAS needs to be extracted from the standard output. Refer to the appropriate documents for guidance.

4. Export the VHD file from the managed disk.

   a. Create a container with the appropriate access level. In this example, a container named `vm-images` with `Container` access level is used.

   b. Get the storage account access key from the Azure portal: **Storage Accounts > *examplesaname* > Access Key > *key1* > *key* > Show > *<copy>***

      You can also use the `az` command for this step.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS
--destination-container $containerName --account-name
$storageAccountName --account-key $storageAccountKey --destination
-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Check the status of the blob copy.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. Download the generated image to your Linux server.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

The URL follows a standard format. For automation, you can derive the URL string as shown below. Alternatively, you can use the Azure CLI `az` command to get the URL.
Example URL:
https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd

7. Clean up the managed disk

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

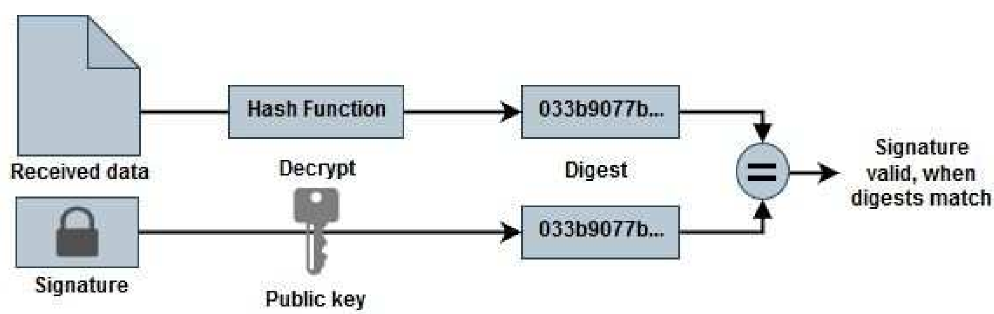
Verify file signature

Azure marketplace image signature verfication for Cloud Volumes ONTAP

The Azure image verification process generates a digest file from the VHD file by stripping 1 MB at the beginning and 512 bytes at the end, then applying a hash function. To match the signing procedure, *sha256* is used for hashing.

File signature verification workflow summary

The following is an overview of the file signature verification workflow process.



- Downloading the Azure image from the NetApp Support Site and extracting the digest (.sig) file, public key certificate (.pem) file, and chain certificate (.pem) file. Refer to Download the Azure image digest file for more information.
- Verification of the chain of trust.
- Extracting the public key (.pub) from the public key certificate (.pem).
- Decrypting the digest file by using the extracted public key.
- Comparing the result against a newly generated digest of a temporary file created from the image file after removing 1 MB at the beginning and 512 bytes at the end. This step is performed by using the OpenSSL command line tool. The OpenSSL CLI tool displays appropriate messaging on success or failure in matching the files.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Verify Azure marketplace image signature for Cloud Volumes ONTAP on Linux

Verification of an exported VHD file signature on Linux includes validating the chain of trust, editing the file, and verifying the signature.

Steps

1. Download the Azure image file from the NetApp Support Site and extract the digest (.sig) file, public key certificate (.pem) file, and chain certificate (.pem) file.

   Refer to Download the Azure image digest file for more information.

2. Verify the chain of trust.

   ```
   % openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem: OK
   ```

3. Remove 1 MB (1,048,576 bytes) at the beginning and 512 bytes at the end of the VHD file. When using `tail`, the `-c +K` option generates bytes from the Kth byte of the file. Therefore, it passes 1048577 to `tail -c`.

   ```
   % tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
   % head -c -512 ./sign.tmp.tail > sign.tmp
   % rm ./sign.tmp.tail
   ```

4. Use OpenSSL to extract the public key from the certificate and verify the stripped file (sign.tmp) with the signature file and the public key.

   The command prompt displays messages indicating success or failure based on the verification.

   ```
   % openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
   ./Code-Sign-Cert-Public-key.pub

   % openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
   -sha256 -signature digest.sig -binary ./sign.tmp
   Verification OK

   % openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
   -sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
   Verification Failure
   ```

5. Clean up the workspace.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Verify Azure marketplace image signature for Cloud Volumes ONTAP on macOS

Verification of an exported VHD file signature on Linux includes validating the chain of trust, editing the file, and verifying the signature.

Steps

1. Download the Azure image file from the NetApp Support Site and extract the digest (.sig) file, public key certificate (.pem) file, and chain certificate (.pem) file.

   Refer to Download the Azure image digest file for more information.

2. Verify the chain of trust.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Remove 1MB (1,048,576 bytes) at the beginning and 512 bytes at the end of the VHD file. When using `tail`, the `-c +K` option generates bytes from the Kth byte of the file. Therefore, it passes 1048577 to `tail -c`. Note that on macOS, the tail command might take about ten minutes to complete.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Use OpenSSL to extract the public key from the certificate and verify the stripped file (sign.tmp) with the signature file and public key. The command prompt displays messages indicating success or failure based on the verification.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Clean up the workspace.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Deploy Cloud Volumes ONTAP from the Azure marketplace

You can use Azure marketplace direct deployment to quickly and easily deploy Cloud Volumes ONTAP. From the Azure marketplace, you can quickly deploy Cloud Volumes ONTAP in a few clicks and explore its core features and capabilities in your environment.

For more information about this offering, refer to Learn about Cloud Volumes ONTAP offerings in the NetApp Console and the marketplace.

About this task

The Cloud Volumes ONTAP system deployed by using Azure marketplace direct deployment has these properties. Note that the features of a standalone instance deployed through the Azure marketplace change when it is discovered in the NetApp Console.

- The latest Cloud Volumes ONTAP version (9.16.1 or later).
- A free license for Cloud Volumes ONTAP that is limited to 500 GiB of provisioned capacity. This license includes no NetApp support and has no expiry date.
- Two nodes configured in a high availability (HA) mode in a single availability zone (AZ), provisioned with default serial numbers. The storage virtual machines (storage VMs) are deployed in a flexible orchestration mode.
- An aggregate for the instance created by default.
- A Premium SSD v2 Managed Disk of 500 GiB provisioned capacity, and a root and a data disk.
- One data storage VM deployed, with NFS, CIFS, iSCSI, and NVMe/TCP data-services. You cannot add any additional data storage VMs.
- Licenses installed for NFS, CIFS (SMB), iSCSI, Autonomous Ransomware Protection (ARP), SnapLock, and SnapMirror.
- ONTAP temperature-sensitive storage efficiency (TSSE), volume encryption, and external key-management enabled by default.
- These features are not supported:
  - FabricPool tiering
  - Changing the storage VM type
  - Fast write mode

Before you begin

- Ensure that you have a valid Azure marketplace subscription.
- Ensure you meet the networking requirements for an HA deployment in a single AZ in Azure. Refer to Set up Azure networking for Cloud Volumes ONTAP.
- You need to be assigned one of these Azure roles to deploy Cloud Volumes ONTAP:
  - The `contributor` role with the default permissions. For more information, refer to the Microsoft Azure

documentation: Azure built-in roles.

◦ A custom RBAC role with the following permissions. For more information, refer to the Azure documentation: Azure custom roles.

```
"permissions": [
{
"actions": [
"Microsoft.AAD/register/action",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Network/loadBalancers/write",
"Microsoft.ClassicCompute/virtualMachines/write",
"Microsoft.Compute/capacityReservationGroups/deploy/action",
"Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGroups/
write",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Network/virtualNetworks/write",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Resources/deployments/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write"
],
"notActions": [],
"dataActions": [],
"notDataActions": []
}
]
```

If you have registered the resource provider "Microsoft.storage" to your subscription, then you don't need the `Microsoft.AAD/register/action` permission. For more information, refer to the Azure documentation: Azure permissions for Storage.

Steps

1. From the Azure marketplace site, search for NetApp products.
2. Select **NetApp Cloud Volumes ONTAP direct**.
3. Click **Create** to launch the deployment wizard.
4. Select a plan. The **Plan** list typically displays the latest releases of Cloud Volumes ONTAP.
5. In the **Basics** tab, provide these details:
   - **Subscription**: Select a subscription. The deployment will be linked to the subscription number.
   - **Resource group**: Use an existing resource group or create a new one. Resource groups help in allocating all resources, such as disks and storage VMs, within a single group for a Cloud Volumes

ONTAP system.

  - **Region**: Select a region that supports Azure HA deployment in a single AZ. You see only the available regions on the list.
  - **Size**: Select an storage VM size for the supported Premium SSD v2 Managed Disk.
  - **Zone**: Select a zone for the region you selected.
  - **Admin Password**: Set a password. You use this admin password to log in to the system after the deployment.
  - **Confirm Password**: Re-enter the same password for confirmation.
    - In the **Network** tab, add a virtual network and a subnet, or select them from the lists.

      > To comply with Microsoft Azure restrictions, you should create a new subnet when setting up a new virtual network. Likewise, if you choose an existing network, you should select an existing subnet.

    - To select a predefined network security group, select **Yes**. Select **No** to assign a predefined Azure network security group with the necessary traffic rules. For more information, refer to Security group rules for Azure.
    - In the **Advanced** tab confirm whether the two Azure features necessary for this deployment have been set. Refer to Enable an Azure feature for Cloud Volumes ONTAP single AZ deployments and Enable high-availability mode for Cloud Volumes ONTAP in Azure.
    - You can define name and value pairs for the resources or resource groups in the **Tags** tab.
    - In the **Review + create** tab, review the details and start the deployment.

After you finish

Select the notification icon to view the progress of your deployment. After Cloud Volumes ONTAP is deployed, you can view the storage VM listed for operations.

Once accessible, use ONTAP System Manager or the ONTAP CLI to log in to the storage VM with the admin credentials that you set. Thereafter, you can create volumes, LUNs, or shares and start utilizing the storage capabilities of Cloud Volumes ONTAP.

Troubleshoot deployment issues

Cloud Volumes ONTAP systems deployed directly through the Azure marketplace do not include support from NetApp. If any issues arise during deployment, you can independently troubleshoot and resolve them.

Steps

1. On the Azure marketplace site, go to **Boot diagnostics > Serial log**.
2. Download and investigate the serial logs.
3. Consult the product documentation and knowledge base (KB) articles for troubleshooting.
   - Azure marketplace documentation
   - NetApp documentation
   - NetApp KB articles

Discover the deployed systems in Console

You can discover the Cloud Volumes ONTAP systems that you deployed using Azure marketplace direct deployment and manage them on the **Systems** page in the Console. The Console agent discovers the systems, adds them and applies the necessary licenses, and unlocks the full capabilities of the Console for these systems. The original HA configuration in a single AZ with PSSD v2 Managed Disks is retained, and the system is registered to the same Azure subscription and resource group as the original deployment.

About this task

On discovering the Cloud Volumes ONTAP systems deployed using Azure marketplace direct deployment, the Console agent performs these tasks:

- Replaces the free licenses of the discovered systems as regular capacity-based Freemium licenses.
- Retains the existing capabilities of the deployed systems, and adds the additional capabilities of the Console, such as data protection, data management, and security features.
- Replaces the installed licenses on the nodes with new ONTAP licenses for NFS, CIFS (SMB), iSCSI, ARP, SnapLock, and SnapMirror.
- Converts the generic node serial numbers to unique serial numbers.
- Assigns new system tags on the resources as required.
- Converts the dynamic IP addresses of the instance to static IP addresses.
- Enables the functionalities of FabricPool tiering, AutoSupport, and write-once-read-many (WORM) storage on the deployed systems. You can activate these features from the Console when you need them.
- Registers the instances to the NSS accounts used to discover them.
- Enables capacity management features in automatic and manual modes for the discovered systems.

Before you begin

Ensure that the deployment is complete on the Azure marketplace. The Console agent can discover the systems only when the deployment is complete and are available for discovery.

Steps

In the Console, you follow the standard procedure for discovering existing systems. Refer to Add an existing Cloud Volumes ONTAP system to the Console.

> During discovery, you might see failure messages, but you can ignore them until the discovery process is complete. Do not modify the system-generated Cloud Volumes ONTAP configurations in the Azure marketplace portal during discovery, especially the system tags. Any changes made to these configurations may lead to unexpected system behavior.

After you finish

After the discovery is complete, you can view the systems listed on the **Systems** page in the Console. You can perform various management tasks, such as expanding the aggregate, adding volumes, provisioning additional storage VMs, and changing the instance types.

Related links

Refer to the ONTAP documentation for more information about creating storage:

- Create volumes for NFS
- Create LUNs for iSCSI
- Create shares for CIFS

Get started in Google Cloud

Quick start for Cloud Volumes ONTAP in Google Cloud

Get started with Cloud Volumes ONTAP in Google Cloud in a few steps.

1

Create a Console agent

If you don't have a Console agent yet, you need to create one. Learn how to create a Console agent in Google Cloud

Note that if you want to deploy Cloud Volumes ONTAP in a subnet where no internet access is available, then you need to manually install the Console agent and access the NetApp Console that's running on that Console agent. Learn how to manually install the Console agent in a location without internet access

2

Plan your configuration

The Console 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 about planning your configuration.

3

Set up your networking

a. Ensure that your VPC and subnets will support connectivity between the Console agent and Cloud Volumes ONTAP.

b. If you plan to enable data tiering, configure the Cloud Volumes ONTAP subnet for Private Google Access.

c. If you're deploying an HA pair, ensure that you have four VPCs, each with their own subnet.

d. If you're using a shared VPC, provide the *Compute Network User* role to the Console agent service account.

e. Enable outbound internet access from the target VPC for NetApp AutoSupport.

   This step isn't required if you're deploying Cloud Volumes ONTAP in a location where no internet access is available.

Learn more about networking requirements.

4

Set up a service account

Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable data tiering to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the NetApp Backup and Recovery to back up volumes to low-cost object storage.

You can set up one service account and use it for both purposes. The service account must have the **Storage Admin** role.

Read step-by-step instructions.

5 Enable Google Cloud APIs

Enable Google Cloud APIs in your project. These APIs, which you might have already enabled as part of creating the Console agent, are required to deploy Cloud Volumes ONTAP in Google Cloud.

6 Launch Cloud Volumes ONTAP using the Console

Click **Add System**, 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 Console agent
- Installing the Console agent software on a Linux host
- Google Cloud permissions for the Console agent

Plan your Cloud Volumes ONTAP configuration in Google Cloud

When you deploy Cloud Volumes ONTAP in Google Cloud, 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 Google Cloud regions. View the full list of supported regions.

Choose a supported machine type

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

Supported configurations for Cloud Volumes ONTAP in Google Cloud

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 Google Cloud

Size your system in Google Cloud

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 machine type, disk type, and disk size:

Machine type

Look at the supported machine types in the Cloud Volumes ONTAP Release Notes and then review details from Google about each supported machine type. Match your workload requirements to the number of vCPUs and memory for the machine type. Note that each CPU core increases networking performance.

Refer to the following for more details:

- Google Cloud documentation: N1 standard machine types
- Google Cloud documentation: Performance

Disk types

When you create volumes for Cloud Volumes ONTAP, you need to choose the underlying cloud storage that Cloud Volumes ONTAP uses for a disk. The disk type can be any of the following:

- *Zonal SSD persistent disks*: SSD persistent disks are best for workloads that require high rates of random IOPS.
- *Zonal Balanced persistent disks*: These SSDs balance performance and cost by providing lower IOPS per GB.
- *Zonal Standard persistent disks* : Standard persistent disks are economical and can handle sequential read/write operations.

  For more details, refer to the Google Cloud documentation: Zonal Persistent disks (Standard and SSD).

Disk size

You need to choose an initial disk size when you deploy a Cloud Volumes ONTAP system. After that you can let the NetApp Console manage a system's capacity for you, but if you want to build aggregates yourself, be aware of the following:

- All disks in an aggregate must be the same size.
- Determine the space that you need, while taking performance into consideration.
- The performance of persistent disks scales automatically with disk size and the number of vCPUs available to the system.

  Refer to the following for more details:

  - Google Cloud documentation: Zonal Persistent disks (Standard and SSD)
  - Google Cloud documentation: Optimizing Persistent Disk and Local SSD Performance

View default system disks

In addition to the storage for user data, the Console 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 Google Cloud.
- Google Cloud docs: Cloud Quotas overview

  Google Cloud Compute Engine enforces quotas on resource usage so you should ensure that you haven't reached your limit before you deploy Cloud Volumes ONTAP.

The Console agent also requires a system disk. View details about the Console agent's default configuration.

Collect networking information

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

Network information for a single-node system

Google Cloud information	Your value
Region	
Zone	
VPC network	
Subnet	
Firewall policy (if using your own)	

Network information for an HA pair in multiple zones

Google Cloud information	Your value
Region	
Zone for Node 1	
Zone for Node 2	
Zone for the mediator	
VPC-0 and subnet	
VPC-1 and subnet	
VPC-2 and subnet	
VPC-3 and subnet	
Firewall policy (if using your own)	

Network information for an HA pair in a single zone

Google Cloud information	Your value
Region	
Zone	
VPC-0 and subnet	
VPC-1 and subnet	
VPC-2 and subnet	
VPC-3 and subnet	

Google Cloud information	Your value
Firewall policy (if using your own)	

Choose a write speed

The Console enables you to choose a write speed setting for Cloud Volumes ONTAP, except for high-availability (HA) pairs in Google Cloud. 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 the Console, 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.

Set up Google Cloud networking for Cloud Volumes ONTAP

The NetApp Console handles the set up of networking components for Cloud Volumes ONTAP, such as IP addresses, netmasks, and routes. You need to make sure that outbound internet access is available, that enough private IP addresses are available, that the right connections are in place, and more.

If you want to deploy an HA pair, you should learn how HA pairs work in Google Cloud.

Requirements for Cloud Volumes ONTAP

The following requirements must be met in Google Cloud.

Requirements specific to single-node systems

If you want to deploy a single-node system, ensure that your networking meets the following requirements.

One VPC

One Virtual Private Cloud (VPC) is required for a single-node system.

Private IP addresses

For a single-node system in Google Cloud, the Console allocates private IP addresses to the following:

- Node
- Cluster
- Storage VM
- Data NAS LIF
- Data iSCSI LIF

You can skip creation of the storage VM (SVM) management LIF if you deploy Cloud Volumes ONTAP using the API and specify the following flag:

```
skipSvmManagementLif: true
```

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

Requirements specific to HA pairs

If you want to deploy an HA pair, ensure that your networking meets the following requirements.

One or multiple zones

You can ensure the high availability of your data by deploying an HA configuration across multiple or in a single zone. The Console prompts you to choose multiple zones or a single zone when you create the HA pair.

- Multiple zones (recommended)

  Deploying an HA configuration across three zones ensures continuous data availability if a failure occurs within a zone. Note that write performance is slightly lower compared to using a single zone, but it's minimal.

- Single zone

  When deployed in a single zone, a Cloud Volumes ONTAP HA configuration uses a spread placement policy. This policy ensures that an HA configuration is protected from a single point of failure within the zone, without having to use separate zones to achieve fault isolation.

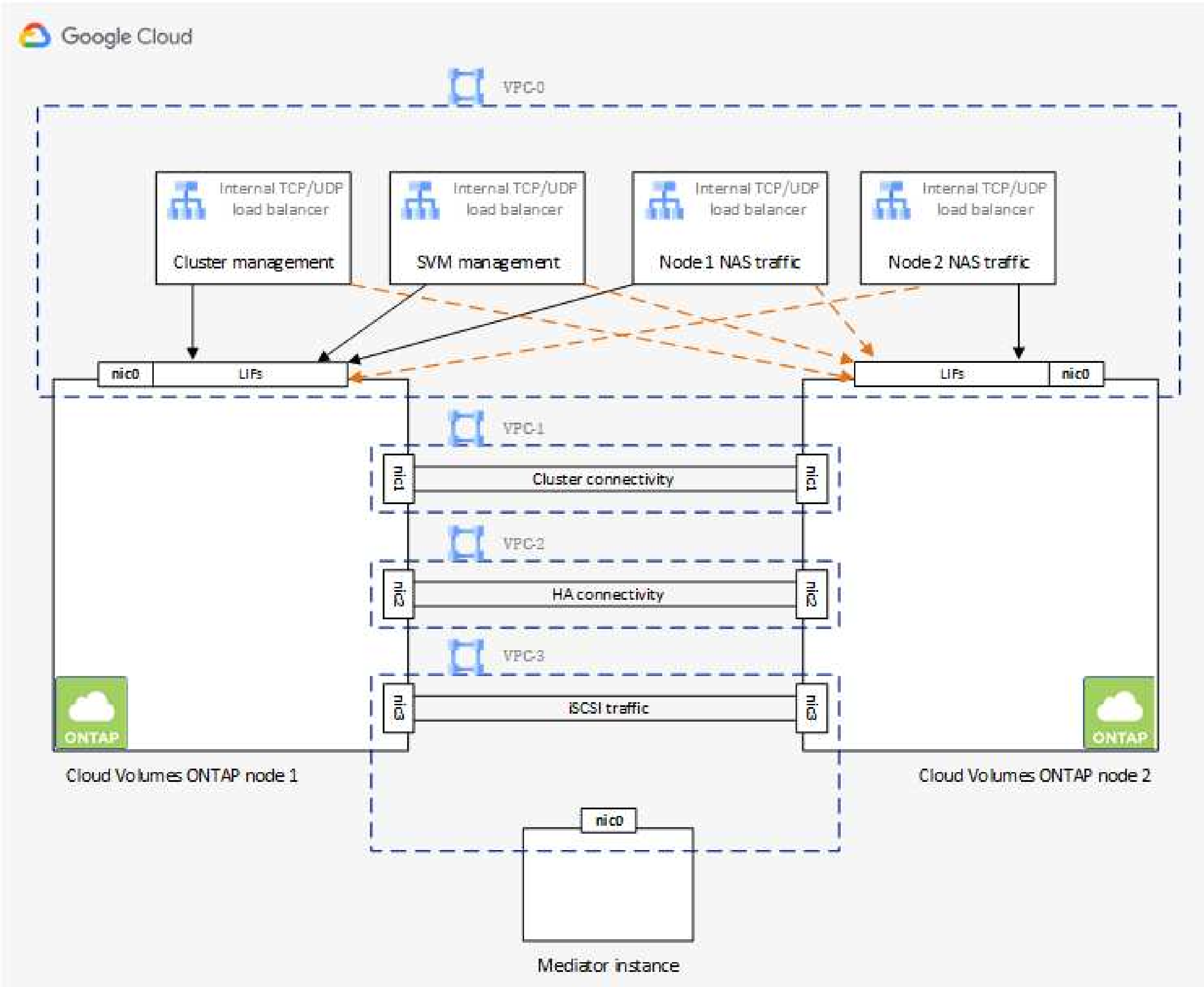
  This deployment model does lower your costs because there are no data egress charges between zones.

Four Virtual Private Clouds

Four Virtual Private Clouds (VPCs) are required for an HA configuration. Four VPCs are required because Google Cloud requires that each network interface resides in a separate VPC network.

The Console prompts you to choose four VPCs when you create the HA pair:

- VPC-0 for inbound connections to the data and nodes
- VPC-1, VPC-2, and VPC-3 for internal communication between the nodes and the HA mediator



Subnets

A private subnet is required for each VPC.

If you place the Console agent in VPC-0, then you will need to enable Private Google Access on the subnet to access the APIs and to enable data tiering.

The subnets in these VPCs must have distinct CIDR ranges. They can’t have overlapping CIDR ranges.

Private IP addresses

The Console automatically allocates the required number of private IP addresses to Cloud Volumes ONTAP in Google Cloud. You need to make sure that your networking has enough private addresses available.

The number of LIFs allocated for Cloud Volumes ONTAP depends on whether you deploy a single-node system or an HA pair. A LIF is an IP address associated with a physical port. An SVM management LIF is required for management tools like SnapCenter.

- **Single node**
  The Console allocates 4 IP addresses to a single-node system:
  - Node management LIF
  - Cluster management LIF
  - iSCSI data LIF

    An iSCSI LIF provides client access over the iSCSI protocol and is used by the system for other important networking workflows. These LIFs are required and should not be deleted.

  - NAS LIF

    You can skip creation of the storage VM (SVM) management LIF if you deploy Cloud Volumes ONTAP using the API and specify the following flag:

    ```
    skipSvmManagementLif: true
    ```

- **HA pair**
  The Console allocates 12-13 IP addresses to an HA pair:
  - 2 Node management LIFs (e0a)
  - 1 Cluster management LIF (e0a)
  - 2 iSCSI LIFs (e0a)

    An iSCSI LIF provides client access over the iSCSI protocol and is used by the system for other important networking workflows. These LIFs are required and should not be deleted.

  - 1 or 2 NAS LIFs (e0a)
  - 2 Cluster LIFs (e0b)
  - 2 HA Interconnect IP addresses (e0c)
  - 2 RSM iSCSI IP addresses (e0d)

    You can skip creation of the storage VM (SVM) management LIF if you deploy Cloud Volumes ONTAP using the API and specify the following flag:

    ```
    skipSvmManagementLif: true
    ```

Internal load balancers

The Console creates four Google Cloud internal load balancers (TCP/UDP) that manage incoming traffic to the Cloud Volumes ONTAP HA pair. No setup is required from your end. We’ve listed this as a requirement simply to inform you of the network traffic and to mitigate any security concerns.

One load balancer is for cluster management, one is for storage VM (SVM) management, one is for NAS traffic to node 1, and the last is for NAS traffic to node 2.

The setup for each load balancer is as follows:

- One shared private IP address
- One global health check

  By default, the ports used by the health check are 63001, 63002, and 63003.

- One regional TCP backend service
- One regional UDP backend service
- One TCP forwarding rule
- One UDP forwarding rule
- Global access is disabled

  Even though global access is disabled by default, enabling it post deployment is supported. We disabled it because cross region traffic will have significantly higher latencies. We wanted to ensure that you didn't have a negative experience due to accidental cross region mounts. Enabling this option is specific to your business needs.

Shared VPCs

Cloud Volumes ONTAP and the Console agent are supported in a Google Cloud shared VPC and also in standalone VPCs.

For a single-node system, the VPC can be either a shared VPC or a standalone VPC.

For an HA pair, four VPCs are required. Each of those VPCs can be either shared or standalone. For example, VPC-0 could be a shared VPC, while VPC-1, VPC-2, and VPC-3 could be standalone VPCs.

A shared VPC enables you to configure and centrally manage virtual networks across multiple projects. You can set up shared VPC networks in the *host project* and deploy the Console agent and Cloud Volumes ONTAP virtual machine instances in a *service project*.

Google Cloud documentation: Shared VPC overview.

Review the required shared VPC permissions covered in Console agent deployment

Packet mirroring in VPCs

Packet mirroring must be disabled in the Google Cloud subnet in which you deploy Cloud Volumes ONTAP.

Outbound internet access

Cloud Volumes ONTAP systems require outbound internet access for accessing external endpoints for various functions. Cloud Volumes ONTAP can't operate properly if these endpoints are blocked in environments with strict security requirements.

The Console agent also contacts several endpoints for day-to-day operations. For information about the endpoints, refer to View endpoints contacted from the Console agent and Prepare networking for using the Console.

Cloud Volumes ONTAP endpoints

Cloud Volumes ONTAP uses these endpoints to communicate with various services.

Endpoints	Applicable for	Purpose	Deployment mode	Impact if endpoint is not available
https://netapp-cloud-account.auth0.com	Authentication	Used for authentication in the Console.	Standard and restricted modes.	User authentication fails and the following services remain unavailable: • Cloud Volumes ONTAP services • ONTAP services • Protocols and proxy services
https://api.bluexp.netapp.com/tenancy	Tenancy	Used to retrieve Cloud Volumes ONTAP resource from the Console to authorize resources and users.	Standard and restricted modes.	Cloud Volumes ONTAP resources and the users are not authorized.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Used to send AutoSupport telemetry data to NetApp support.	Standard and restricted modes.	AutoSupport information remains undelivered.
https://cloudbuild.googleapis.com/v1 (for only private mode deployments) https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud (Commercial use).	Communication with Google Cloud services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Google Cloud service to perform specific operations for the Console in Google Cloud.

Connections to ONTAP systems in other networks

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

Google Cloud documentation: Cloud VPN overview.

Firewall rules

The Console creates Google Cloud firewall rules 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 to use your own firewall rules.

The firewall rules for Cloud Volumes ONTAP requires both inbound and outbound rules. If you're deploying an HA configuration, these are the firewall rules for Cloud Volumes ONTAP in VPC-0.

Note that two sets of firewall rules are required for an HA configuration:

- One set of rules for HA components in VPC-0. These rules enable data access to Cloud Volumes ONTAP.
- Another set of rules for HA components in VPC-1, VPC-2, and VPC-3. These rules are open for inbound & outbound communication between the HA components. Learn more.

Looking for information about the Console agent? View firewall rules for the Console agent

Inbound rules

When you add a Cloud Volumes ONTAP system, you can choose the source filter for the predefined firewall policy during deployment:

- **Selected VPC only**: the source filter for inbound traffic is the subnet range of the VPC for the Cloud Volumes ONTAP system and the subnet range of the VPC where the Console agent resides. This is the recommended option.
- **All VPCs**: the source filter for inbound traffic is the 0.0.0.0/0 IP range.

If you use your own firewall policy, ensure that you add all networks that need to communicate with Cloud Volumes ONTAP, but also ensure to add both address ranges to allow the internal Google Load Balancer to function correctly. These addresses are 130.211.0.0/22 and 35.191.0.0/16. For more information, refer to the Google Cloud documentation: Load Balancer Firewall Rules.

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
HTTP	80	HTTP access to the ONTAP System Manager web console using the IP address of the cluster management LIF
HTTPS	443	Connectivity with the Console agent and HTTPS access to the ONTAP System Manager web console using the IP address of the cluster management LIF
SSH	22	SSH access to the IP address of the cluster management LIF or a node management LIF
TCP	111	Remote procedure call for NFS
TCP	139	NetBIOS service session for CIFS

Protocol	Port	Purpose
TCP	161-162	Simple network management protocol
TCP	445	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	635	NFS mount
TCP	749	Kerberos
TCP	2049	NFS server daemon
TCP	3260	iSCSI access through the iSCSI data LIF
TCP	4045	NFS lock daemon
TCP	4046	Network status monitor for NFS
TCP	10000	Backup using NDMP
TCP	11104	Management of intercluster communication sessions for SnapMirror
TCP	11105	SnapMirror data transfer using intercluster LIFs
TCP	63001-63050	Load balance probe ports to determine which node is healthy (required for HA pairs only)
UDP	111	Remote procedure call for NFS
UDP	161-162	Simple network management protocol
UDP	635	NFS mount
UDP	2049	NFS server daemon
UDP	4045	NFS lock daemon
UDP	4046	Network status monitor for NFS
UDP	4049	NFS rquotad protocol

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.

Protocol	Port	Purpose
All ICMP	All	All outbound traffic
All TCP	All	All outbound traffic
All UDP	All	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 Cloud Volumes ONTAP clusters use the following ports for regulating nodes traffic.

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

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

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

Rules for VPC-1, VPC-2, and VPC-3

In Google Cloud, an HA configuration is deployed across four VPCs. The firewall rules needed for the HA configuration in VPC-0 are listed above for Cloud Volumes ONTAP.

Meanwhile, the predefined firewall rules created for the instances in VPC-1, VPC-2, and VPC-3 enable ingress communication over *all* protocols and ports. These rules enable communication between HA nodes.

Communication from the HA nodes to the HA mediator takes place over port 3260 (iSCSI).

> To enable high write speed for new Google Cloud HA pair deployments, a maximum transmission unit (MTU) of at least 8,896 bytes is required for VPC-1, VPC-2, and VPC-3. If you choose to upgrade existing VPC-1, VPC-2, and VPC-3 to an MTU of 8,896 bytes, you must shutdown all existing HA systems using these VPCs during the configuration process.

Infrastructure Manager configuration for private mode deployments

If you want to deploy Cloud Volumes ONTAP 9.16.1 or later in private mode, you need to make a few configuration changes so that Cloud Volumes ONTAP can use Google Cloud Infrastructure Manager as the deployment service instead of Deployment Manager, which Google will eventually deprecate.

Before you begin

- Ensure that your Cloud Volumes ONTAP system is 9.16.1 or later. If it isn't, upgrade your system. Refer to Upgrade Cloud Volumes ONTAP for instructions.
- Ensure that the Google Cloud APIs are enabled. Refer to Enable Google Cloud APIs.
- Ensure that the Cloud Build API is enabled. Refer to Enable the Cloud Build API here.
- Verify that the Console agent's service account has all standard permissions. Additionally, ensure that the service account has the `cloudbuild.workerpools.get` and `cloudbuild.workerpools.list` permissions. Refer to Google Cloud permissions for the Console agent.

Steps

1. Create a private worker pool with this configuration in the same region as the Cloud Volumes ONTAP deployments. For information about creating a private worker pool, refer to Google Cloud documentation: Create and manage private pools and Google Cloud Build pricing.

   The worker pool must have the following configuration:

   - Machine type: e2-medium
   - Disk size: 100 GB
   - Assign external IP: False
   - Network: Default or a private.
   - The subnet configured to access Google APIs. Perform these steps to ensure that the subnet can access Google APIs:
     a. Ensure "Private Google Access" is turned on for the subnet.
     b. Go to **VPC Network level > Private Service Access Tab > Allocated IP ranges for services**.
     c. Select **Allocate IP range** and allocate the internal IP range for the private connection to the Google Compute Service.
     d. On **Private connection to services**, select **Create Connection**.

   e. Select **Connected service producer = Google Cloud Platform**.
   f. Assign the allocation for the private connection IP range you created in the previous step.
2. Deploy this worker pool and keep it running for Cloud Volumes ONTAP management. Google Cloud uses this worker pool to run all Terraform operations in an isolated environment.
3. When deploying Cloud Volumes ONTAP in private mode, select the name of this worker pool in the **GCP Worker Pool** field. Refer to Launch Cloud Volumes ONTAP in Google Cloud for instructions.

Requirements for the Console agent

If you haven't created a Console agent yet, you should review networking requirements.

- View networking requirements for the Console agent
- Firewall rules in Google Cloud

Network configurations to support Console agent proxy

You can use the proxy servers configured for the Console agent to enable outbound internet access from Cloud Volumes ONTAP. The Console supports two types of proxies:

- **Explicit proxy**: The outbound traffic from Cloud Volumes ONTAP uses the HTTP address of the proxy server specified during the Console agent proxy configuration. The Console agent administrator might also have configured user credentials and root CA certificates for additional authentication. If a root CA certificate is available for the explicit proxy, make sure to obtain and upload the same certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.
- **Transparent proxy**: The network is configured to automatically route outbound traffic from Cloud Volumes ONTAP through the Console agent proxy. When setting up a transparent proxy, the Console agent administrator needs to provide only a root CA certificate for connectivity from Cloud Volumes ONTAP, not the HTTP address of the proxy server. Make sure that you obtain and upload the same root CA certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.

For information about configuring proxy servers for the Console agent, refer to the Configure a Console agent to use a proxy server.

Configure network tags for Cloud Volumes ONTAP in Google Cloud

During the transparent proxy configuration of the Console agent, the administrator adds a network tag for Google Cloud. You need to obtain and manually add the same network tag for your Cloud Volumes ONTAP configuration. This tag is necessary for the proxy server to function correctly.

1. In the Google Cloud Console, locate your Cloud Volumes ONTAP system.
2. Go to **Details > Networking > Network tags**.
3. Add the tag used for the Console agent and save the configuration.

Related topics

- Verify AutoSupport setup for Cloud Volumes ONTAP
- Learn about ONTAP internal ports.

Set up VPC Service Controls to deploy Cloud Volumes ONTAP in Google Cloud

When choosing to lock down your Google Cloud environment with VPC Service Controls, you should understand how NetApp Console and Cloud Volumes ONTAP interact with the

Google Cloud APIs, as well as how to configure your service perimeter to deploy the Console and Cloud Volumes ONTAP.

VPC Service Controls enable you to control access to Google-managed services outside of a trusted perimeter, to block data access from untrusted locations, and to mitigate unauthorized data transfer risks. Learn more about Google Cloud VPC Service Controls.

How NetApp services communicate with VPC Service Controls

The Console communicates directly with the Google Cloud APIs. This is either triggered from an external IP address outside of Google Cloud (for example, from api.services.cloud.netapp.com), or within Google Cloud from an internal address assigned to the Console agent.

Depending on the deployment style of the Console agent, certain exceptions may have to be made for your service perimeter.

Images

Both Cloud Volumes ONTAP and the Console use images from a project within Google Cloud that is managed by NetApp. This can affect the deployment of the Console agent and Cloud Volumes ONTAP, if your organization has a policy that blocks the use of images that are not hosted within the organization.

You can deploy a Console agent manually using the manual installation method, but Cloud Volumes ONTAP will also need to pull images from the NetApp project. You must provide an allowed list in order to deploy a Console agent and Cloud Volumes ONTAP.

Deploying a Console agent

The user who deploys a Console agent needs to be able to reference an image hosted in the projectId *netapp-cloudmanager* and the project number *14190056516*.

Deploying Cloud Volumes ONTAP

- The Console service account needs to reference an image hosted in the projectId *netapp-cloudmanager* and the project number *14190056516* from the service project.
- The service account for the default Google APIs Service Agent needs to reference an image hosted in the projectId *netapp-cloudmanager* and the project number *14190056516* from the service project.

Examples of the rules needed for pulling these images with VPC Service Controls are defined below.

VPC Service Controls perimeter policies

Policies allow exceptions to the VPC Service Controls rule sets. For more information about policies, please visit the Google Cloud VPC Service Controls Policy Documentation.

To set the policies that the Console requires, navigate to your VPC Service Controls Perimeter within your organization and add the following policies. The fields should match the options given in the VPC Service Controls policy page. Also note that **all** rules are required and the **OR** parameters should be used in the rule set.

Ingress rules

Rule 1

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

OR

Rule 2

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

OR

Rule 3

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Egress rules

Rule 1:

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

> The project number outlined above is the project *netapp-cloudmanager* used by NetApp to store images for the Console agent and for Cloud Volumes ONTAP.

Create a Google Cloud service account for Cloud Volumes ONTAP

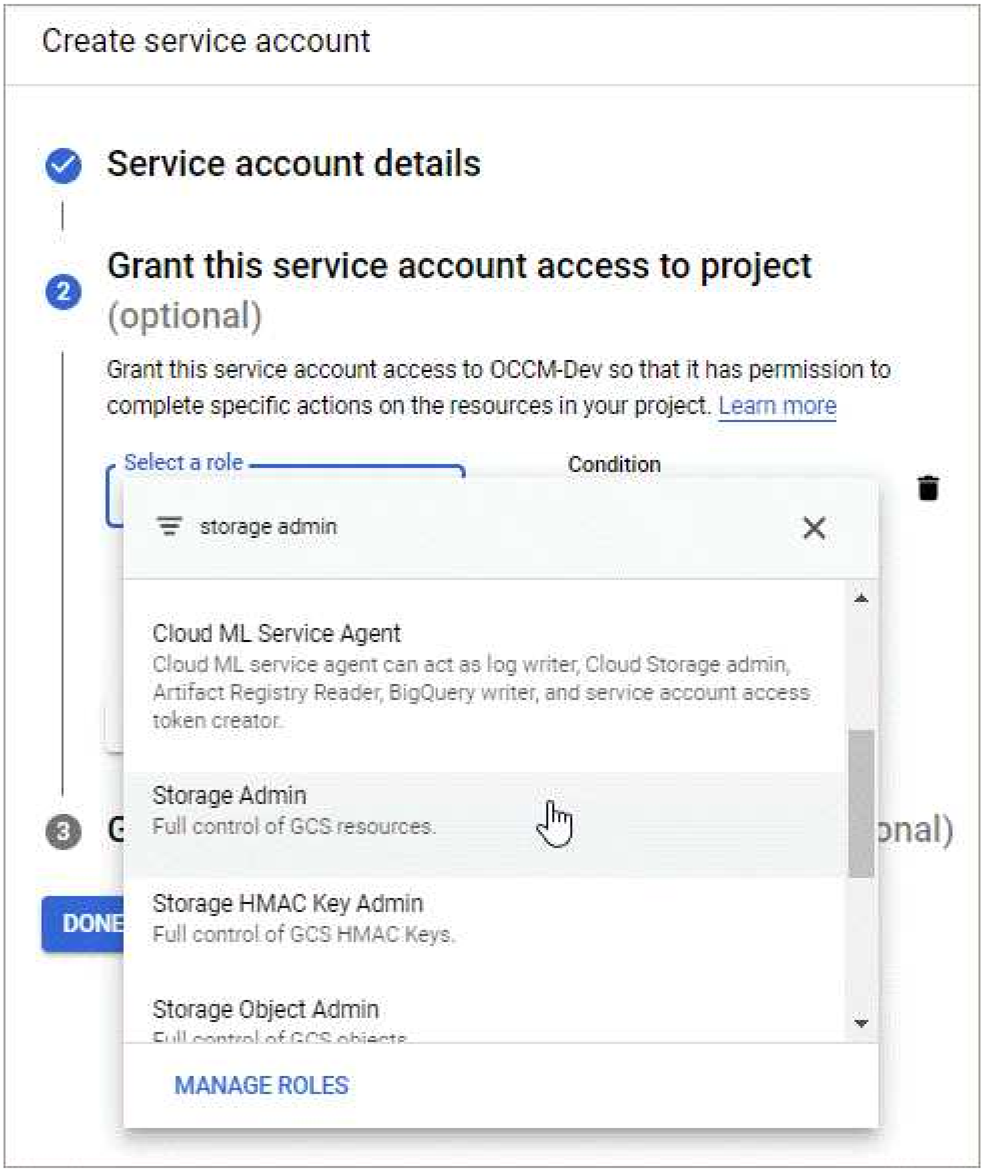
Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable data tiering to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the NetApp Backup and Recovery to back up volumes to low-cost object storage.

Cloud Volumes ONTAP uses the service account to access and manage one bucket for tiered data and another bucket for backups.

You can set up one service account and use it for both purposes. The service account must have the **Storage Admin** role.

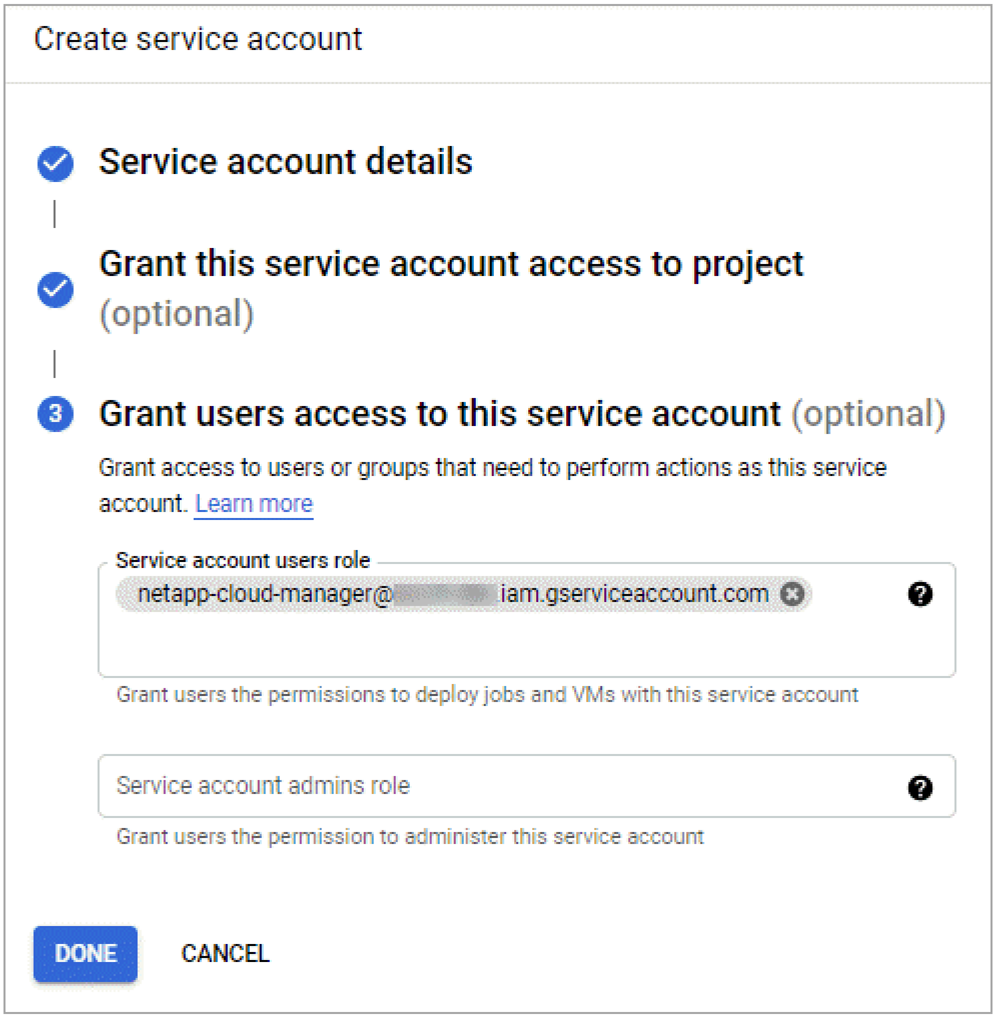
Steps

1. In the Google Cloud Console, go to the Service accounts page.
2. Select your project.
3. Click **Create service account** and provide the required information.
   a. **Service account details**: Enter a name and description.
   b. **Grant this service account access to project**: Select the **Storage Admin** role.



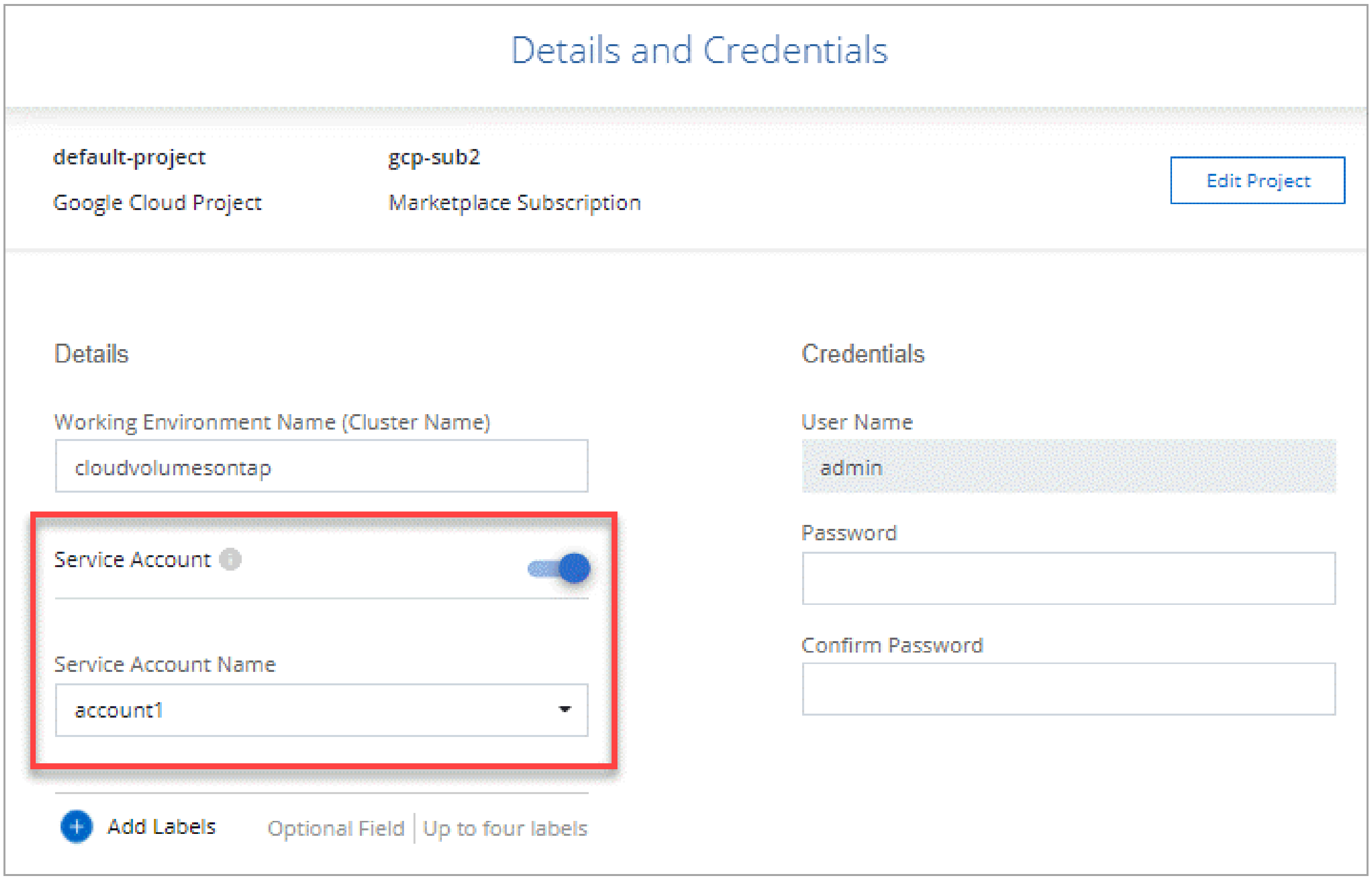
c. **Grant users access to this service account**: Add the Console agent service account as a *Service Account User* to this new service account.

This step is required for data tiering only. It's not required for Backup and Recovery.



What's next?

You'll need to select the service account later when you create a Cloud Volumes ONTAP system.



Using customer-managed encryption keys with Cloud Volumes ONTAP

While Google Cloud Storage always encrypts your data before it's written to disk, you can use the APIs to create a Cloud Volumes ONTAP system that uses *customer-managed encryption keys*. These are keys that you generate and manage in GCP using the Cloud Key Management Service.

Steps

1. Ensure that the Console agent service account has the correct permissions at the project level, in the project where the key is stored.

   The permissions are provided in the the service account permissions by default, but may not be applied if you use an alternate project for the Cloud Key Management Service.

   The permissions are as follows:

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. Ensure that the service account for the Google Compute Engine Service Agent has Cloud KMS Encrypter/Decrypter permissions on the key.

The name of the service account uses the following format: "service-[service_project_number]@compute-system.iam.gserviceaccount.com".

Google Cloud Documentation: Using IAM with Cloud KMS - Granting roles on a resource

3. Obtain the "id" of the key by invoking the get command for the `/gcp/vsa/metadata/gcp-encryption-keys` API call or by choosing "Copy Resource Name" on the key in the GCP console.
4. If using customer-managed encryption keys and tiering data to object storage, the NetApp Console attempts to utilize the same keys that are used to encrypt the persistent disks. But you'll first need to enable Google Cloud Storage buckets to use the keys:
   a. Find the Google Cloud Storage service agent by following the Google Cloud Documentation: Getting the Cloud Storage service agent.
   b. Navigate to the encryption key and assign the Google Cloud Storage service agent with Cloud KMS Encrypter/Decrypter permissions.

   For more information, refer to Google Cloud Documentation: Using customer-managed encryption keys
5. Use the "gcpEncryption" parameter with your API request when creating a system.

   Example

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-
1/cryptoKeys/generatedkey1"
  }
```

Refer to the NetApp Console automation docs for more details about using the "GcpEncryption" parameter.

Set up licensing for Cloud Volumes ONTAP in Google Cloud

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 system.

Freemium

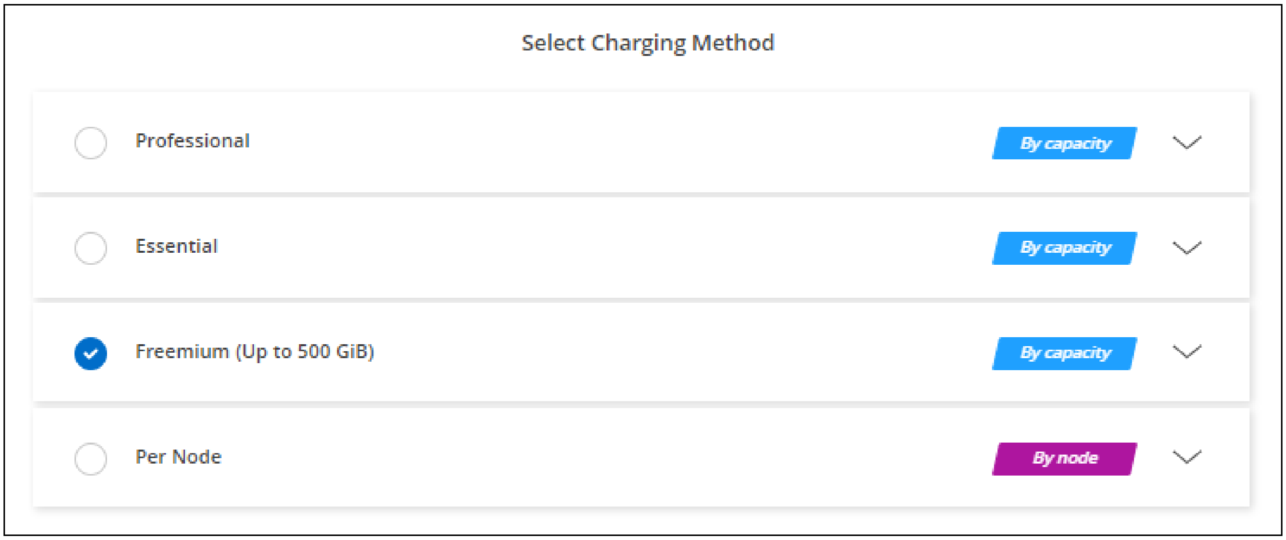
Select the Freemium offering to use Cloud Volumes ONTAP free of charge with up to 500 GiB of provisioned capacity. Learn more about the Freemium offering.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the steps in the NetApp Console.
   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 Google Cloud 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 the Console, select **Freemium** when you reach the charging methods page.



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

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 or Professional package.

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

- A license (bring your own license (BYOL)) purchased from NetApp
- An hourly, pay-as-you-go (PAYGO) subscription from the Google Cloud 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.

> NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP.

Steps

1. Contact NetApp Sales to obtain a license
2. Add your NetApp Support Site account to the NetApp Console

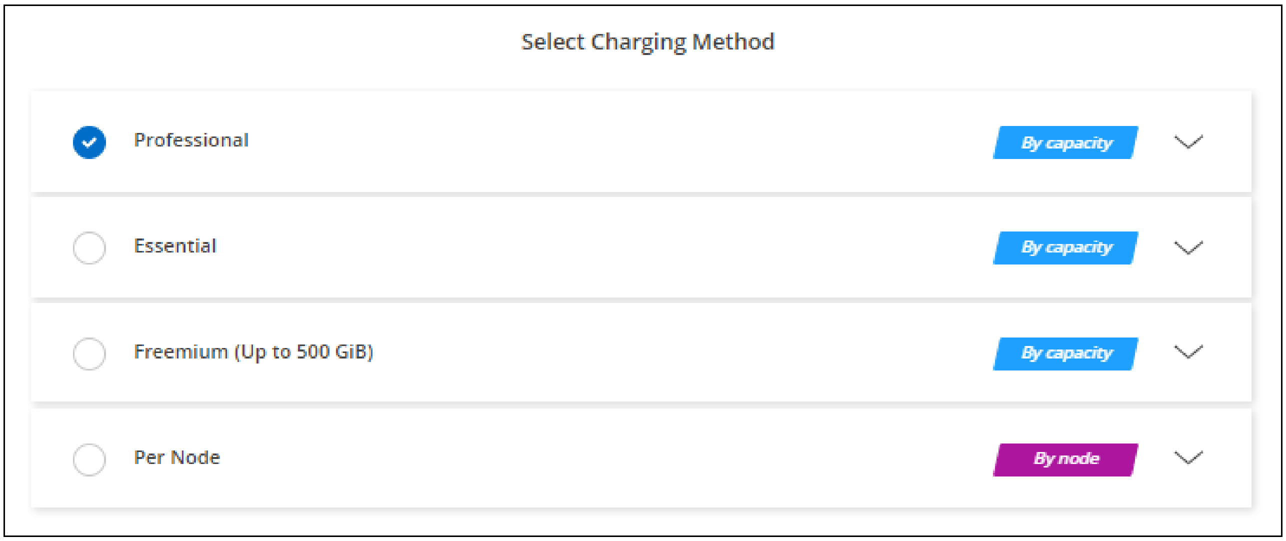
   The Console automatically queries NetApp's licensing service to obtain details about the licenses associated with your NetApp Support Site account. If there are no errors, the Console adds the licenses.

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

3. On the **Systems** page, click **Add System** and follow the steps.
   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 Google Cloud 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 the Console, select a capacity-based package when you reach the charging methods page.



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

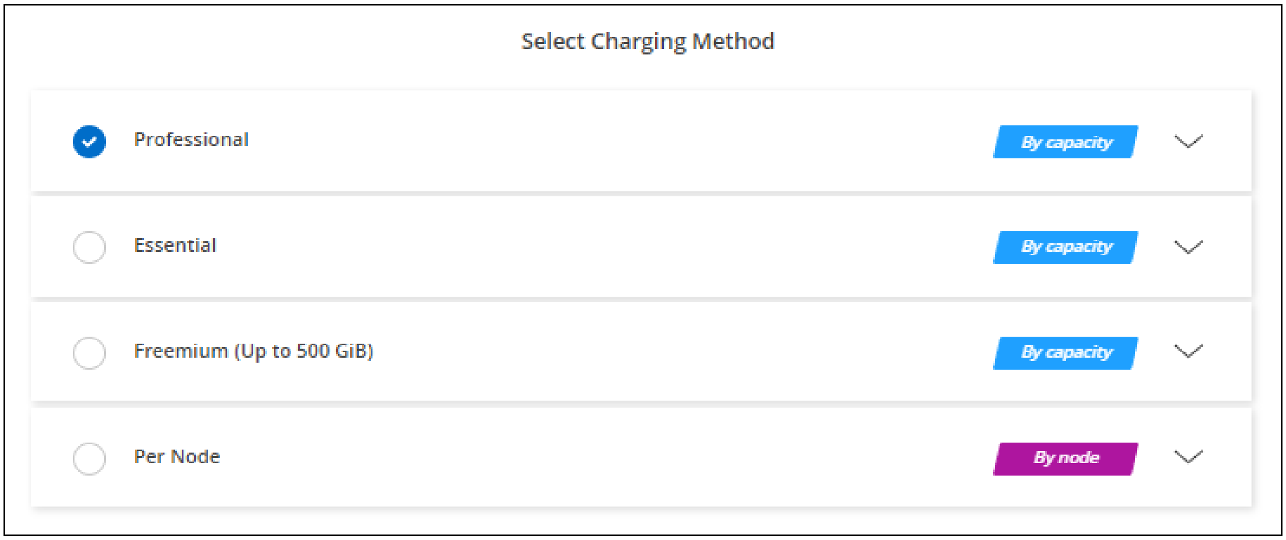
PAYGO subscription

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

When you create a Cloud Volumes ONTAP system, the Console prompts you to subscribe to the agreement that's available in the Google Cloud Marketplace. That subscription is then associated with the system for charging. You can use that same subscription for additional systems.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the steps.
   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 Google Cloud Marketplace.
   b. After you return to the Console, select a capacity-based package when you reach the charging methods page.



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

> You can manage the Google Cloud Marketplace subscriptions associated with your accounts from the Settings > Credentials page. Learn how to manage your Google Cloud credentials 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 Google Cloud Marketplace.

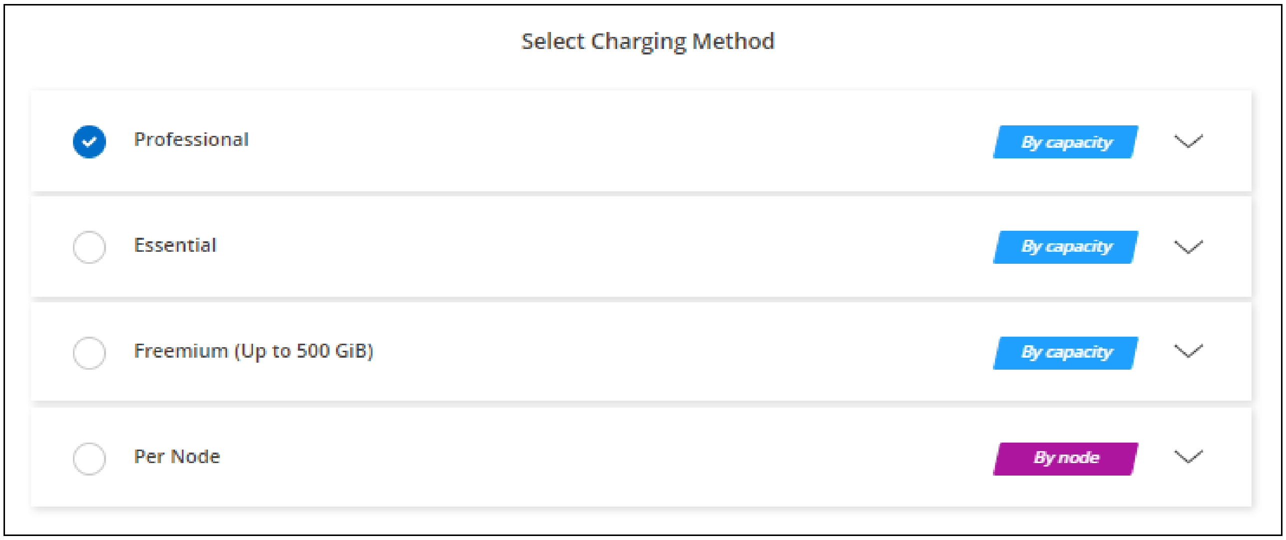
   After NetApp shares the private offer with you, you can select the annual plan when you subscribe from the Google Cloud Marketplace during system creation.

2. On the **Systems** page, click **Add System** and follow the steps.

   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the annual plan in the Google Cloud Marketplace.

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

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



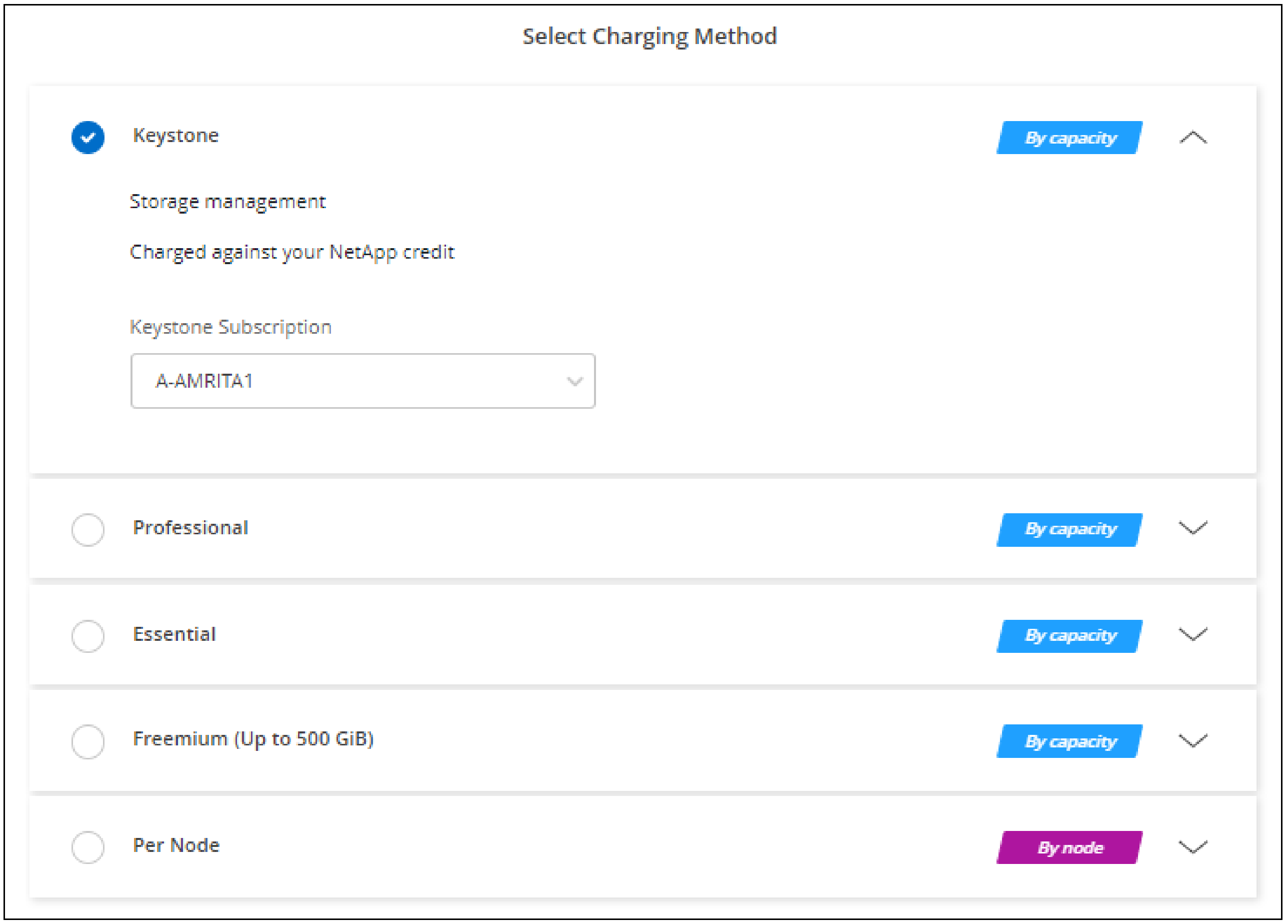
View step-by-step instructions to launch Cloud Volumes ONTAP in Google Cloud.

Keystone Subscription

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

Steps

1. If you don't have a subscription yet, contact NetApp
2. Contact NetApp to authorize your the Console user account with one or more Keystone Subscriptions.
3. After NetApp authorizes your account, link your subscriptions for use with Cloud Volumes ONTAP.
4. On the **Systems** page, click **Add System** and follow the steps.
    a. Select the Keystone Subscription charging method when prompted to choose a charging method.



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

Node-based license

A node-based license is the previous generation license for Cloud Volumes ONTAP. A node-based license could be procured from NetApp (BYOL) and is available for license renewals, only in specific cases. For information, refer to:

- End of availability for node-based licenses
- End of availability of node-based licenses
- Convert a node-based license to a capacity-based license

Launch Cloud Volumes ONTAP in Google Cloud

You can launch Cloud Volumes ONTAP in a single-node configuration or as an HA pair in Google Cloud.

Before you begin

You need the following before you begin.

- A NetApp Console agent that's up and running.
  - You should have a Console agent that is associated with your system.
  - You should be prepared to leave the Console agent running at all times.

    - The service account associated with the Console agent should have the required permissions

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

  You should have prepared by choosing a configuration and by obtaining Google Cloud networking information from your administrator. For details, refer to 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.

- Google Cloud APIs should be enabled in your project:
    - Cloud Deployment Manager V2 API
    - Cloud Logging API
    - Cloud Resource Manager API
    - Compute Engine API
    - Identity and Access Management (IAM) API

Launch a single-node system in Google Cloud

Create a system in the NetApp Console to launch Cloud Volumes ONTAP in Google Cloud.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the prompts.
3. **Choose a Location**: Select **Google Cloud** and **Cloud Volumes ONTAP**.
4. If you're prompted, create a Console agent.
5. **Details & Credentials**: Select a project, specify a cluster name, optionally select a service account, optionally add labels, and then specify credentials.

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

Field	**Description**
System Name	The Console uses the system name to name both the Cloud Volumes ONTAP system and the Google Cloud VM instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Service Account Name	If you plan to use data tiering or NetApp Backup and Recovery with Cloud Volumes ONTAP, then you need to enable **Service Account** and select a service account that has the predefined Storage Admin role. Learn how to create a service account.

Field	Description
Add Labels	Labels are metadata for your Google Cloud resources. The Console adds the labels to the Cloud Volumes ONTAP system and Google Cloud resources associated with the system. You can add up to four labels from the user interface when creating a system, and then you can add more after it's created. Note that the API does not limit you to four labels when creating a system. For information about labels, refer to the Google Cloud Documentation: Labeling Resources.
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 ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Project	Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where of the Console. If you don't see any additional projects in the drop-down list, then you haven't yet associated the service account with other projects. Go to the Google Cloud Console, open the IAM service, and select the project. Add the service account with the role that you use for the Console to that project. You'll need to repeat this step for each project. This is the service account that you set up for the Console, as described on this page. Click **Add Subscription** to associate the selected credentials with a subscription. To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a Google Cloud project that's associated with a subscription to Cloud Volumes ONTAP from the Google Cloud marketplace. Refer to Associating a marketplace subscription with Google Cloud credentials.

6. **Services**: Select the services that you want to use on this system. In order to select Backup and Recovery, or to use NetApp Cloud Tiering, you must have specified the Service Account in step 3.

   If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

7. **Location & Connectivity**: Select the Google Cloud region and zone for your system, choose a firewall policy, and confirm network connectivity to Google Cloud storage for data tiering.

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

Field	Description
Connectivity verification	To tier cold data to a Google Cloud Storage bucket, the subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access. For instructions, refer to Google Cloud Documentation: Configuring Private Google Access.
Generated firewall policy	If you let the Console generate the firewall policy for you, you need to choose how you'll allow traffic: • If you choose **Selected VPC only**, the source filter for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Console agent resides. This is the recommended option. • If you choose **All VPCs**, the source filter for inbound traffic is the 0.0.0.0/0 IP range.
Use existing firewall policy	If you use an existing firewall policy, ensure that it includes the required rules: Learn about firewall rules for Cloud Volumes ONTAP

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**. The preconfigured packages vary with the selected Cloud Volumes ONTAP version. For example, for Cloud Volumes ONTAP 9.18.1 and later, the Console shows packages with C3 VMs, including Hyperdisk Balanced disks. You can modify the configurations, such as IOPS and throughput parameters, based on your workload needs.

   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 machine type.

    > If a newer Release Candidate, General Availability, or patch release is available for a selected version, then the Console updates the system to that version when creating it. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another— for example, from 9.13 to 9.14.
11. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type and the size for each disk.

    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 the Console 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, refer to Size your system in Google Cloud.
12. **Flash Cache, Write Speed & WORM**:

a. Enable **Flash Cache** or choose **Normal** or **High** write speed if you need.

   Learn more about Flash Cache and write speed.

   > High write speed and a higher maximum transmission unit (MTU) of 8,896 bytes are available through the **High** write speed option. In addition, the higher MTU of 8,896 requires the selection of VPC-1, VPC-2 and VPC-3 for the deployment. For more information on VPC-1, VPC-2, and VPC-3, refer to Rules for VPC-1, VPC-2, and VPC-3.

b. Activate write once, read many (WORM) storage, if desired.

   WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

   Learn more about WORM storage.

c. If you activate WORM storage, select the retention period.

13. **Data Tiering in Google Cloud Platform**: Choose whether to enable data tiering on the initial aggregate, choose a storage class for the tiered data, and then either select a service account that has the predefined Storage Admin role (required for Cloud Volumes ONTAP 9.7 or later), or select a Google Cloud account (required for Cloud Volumes ONTAP 9.6).

    Note the following:

    - The Console sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Console agent service account as a user of the tiering service account, otherwise, you can't select it from the Console.
    - For help with adding a Google Cloud account, refer to Setting up and adding Google Cloud accounts for data tiering with 9.6.
    - 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, but you'll need to turn off the system and add a service account from the Google Cloud Console.

      Learn more about data tiering.

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

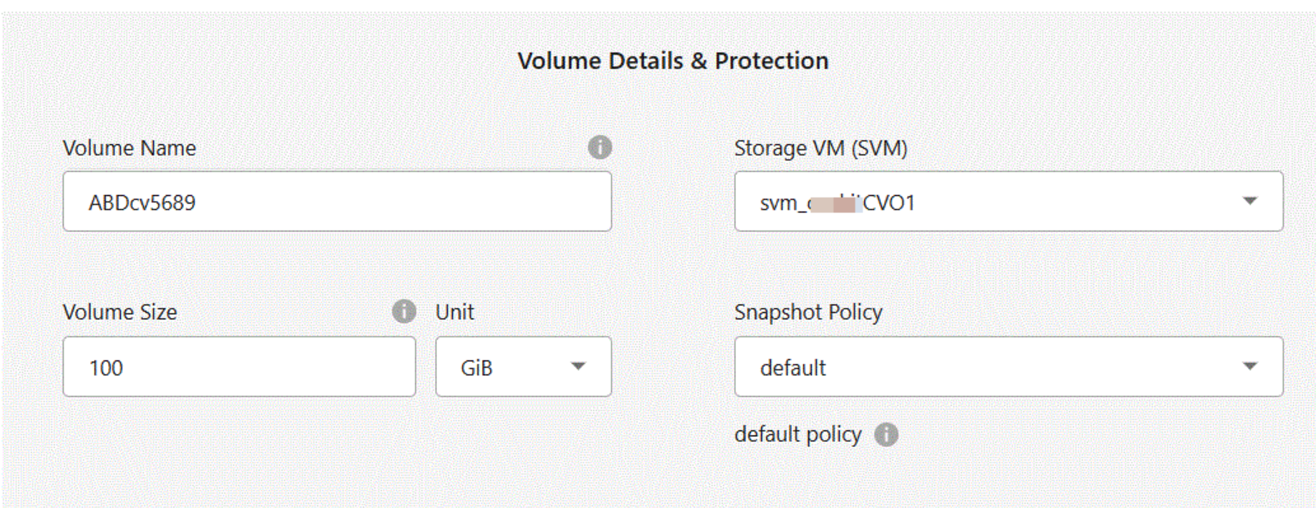
    Learn about supported client protocols and versions.

    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, the Console enters a value that provides access to all instances in the subnet.

Field	Description
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, the Console 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 first page of the volume creation wizard:



15. **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. If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.
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 Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=Cloud** in this field. Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD
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. For information, refer to the NetApp Console 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.

16. **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, refer to Choose a volume usage profile, Data tiering overview, and KB: What Inline Storage Efficiency features are supported with CVO?

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

    a. Review details about the configuration.

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

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

    d. Click **Go**.

Result

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the **Audit** page.

If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the system 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 ONTAP System Manager or the ONTAP CLI.

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

> After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Google Cloud portal, such as the system tags, and the labels set in the Google Cloud resources. Any changes made to these configurations may lead to unexpected behavior or data loss.

Launch an HA pair in Google Cloud

Create a system in the Console to launch Cloud Volumes ONTAP in Google Cloud.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Storage > System** and follow the prompts.
3. **Choose a Location**: Select **Google Cloud** and **Cloud Volumes ONTAP HA**.
4. **Details & Credentials**: Select a project, specify a cluster name, optionally select a Service Account, optionally add labels, and then specify credentials.

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

Field	Description
System Name	The Console uses the system name to name both the Cloud Volumes ONTAP system and the Google Cloud VM instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Service Account Name	If you plan to use the NetApp Cloud Tiering or Backup and Recovery services, you need to enable the **Service Account** switch and then select the Service Account that has the predefined Storage Admin role.
Add Labels	Labels are metadata for your Google Cloud resources. The Console adds the labels to the Cloud Volumes ONTAP system and Google Cloud resources associated with the system. You can add up to four labels from the user interface when creating a system, and then you can add more after it's created. Note that the API does not limit you to four labels when creating a system. For information about labels, refer to Google Cloud Documentation: Labeling 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 ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
Edit Project	Select the project where you want Cloud Volumes ONTAP to reside. If you don't see any additional projects in the drop-down list, then you haven't yet associated the service account with other projects. Go to the Google Cloud Console, open the IAM service, and select the project. Add the service account with the role that you use for the Console to that project. You'll need to repeat this step for each project. This is the service account that you set up for the Console, as described on this page. Click **Add Subscription** to associate the selected credentials with a subscription. To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a Google Cloud project that's associated with a subscription to Cloud Volumes ONTAP from the Google Cloud Marketplace. Refer to Associating a marketplace subscription with Google Cloud credentials.

5. **Services**: Select the services that you want to use on this system. To select Backup and Recovery, or to use NetApp Cloud Tiering, you must have specified the Service Account in step 3.

   If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

6. **HA Deployment Models**: Choose multiple zones (recommended) or a single zone for the HA configuration. Then select a region and zone.

   Learn more about HA deployment models.

7. **Connectivity**: Select four different VPCs for the HA configuration, a subnet in each VPC, and then choose a firewall policy.

   Learn more about networking requirements.

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

Field	Description
Generated policy	If you let the Console generate the firewall policy for you, you need to choose how you'll allow traffic: • If you choose **Selected VPC only**, the source filter for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Console agent resides. This is the recommended option. • If you choose **All VPCs**, the source filter for inbound traffic is the 0.0.0.0/0 IP range.
Use existing	If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.

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 machine type.

    > If a newer Release Candidate, General Availability, or patch release is available for the selected version, then the Console updates the system to that version when creating it. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another—for example, from 9.13 to 9.14.
11. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type and the size for each disk.

    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 the Console 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, refer to Size your system in Google Cloud.
12. **Flash Cache, Write Speed & WORM**:
    a. Enable **Flash Cache** or choose **Normal** or **High** write speed if you need.

       Learn more about Flash Cache and write speed.

> High write speed and a higher maximum transmission unit (MTU) of 8,896 bytes are available through the **High** write speed option with the n2-standard-16, n2-standard-32, n2-standard-48, and n2-standard-64 instance types. In addition, the higher MTU of 8,896 requires the selection of VPC-1, VPC-2 and VPC-3 for the deployment. High write speed and an MTU of 8,896 are feature-dependent and cannot be disabled individually within a configured instance. For more information on VPC-1, VPC-2, and VPC-3, refer to Rules for VPC-1, VPC-2, and VPC-3.

b. Activate write once, read many (WORM) storage, if desired.

   WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

   Learn more about WORM storage.

c. If you activate WORM storage, select the retention period.

13. **Data Tiering in Google Cloud**: Choose whether to enable data tiering on the initial aggregate, choose a storage class for the tiered data, and then select a service account that has the predefined Storage Admin role.

    Note the following:

    - The Console sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Console agent service account as a user of the tiering service account, otherwise, you can't select it from the Console.
    - 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, but you'll need to turn off the system and add a service account from the Google Cloud Console.

      Learn more about data tiering.

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

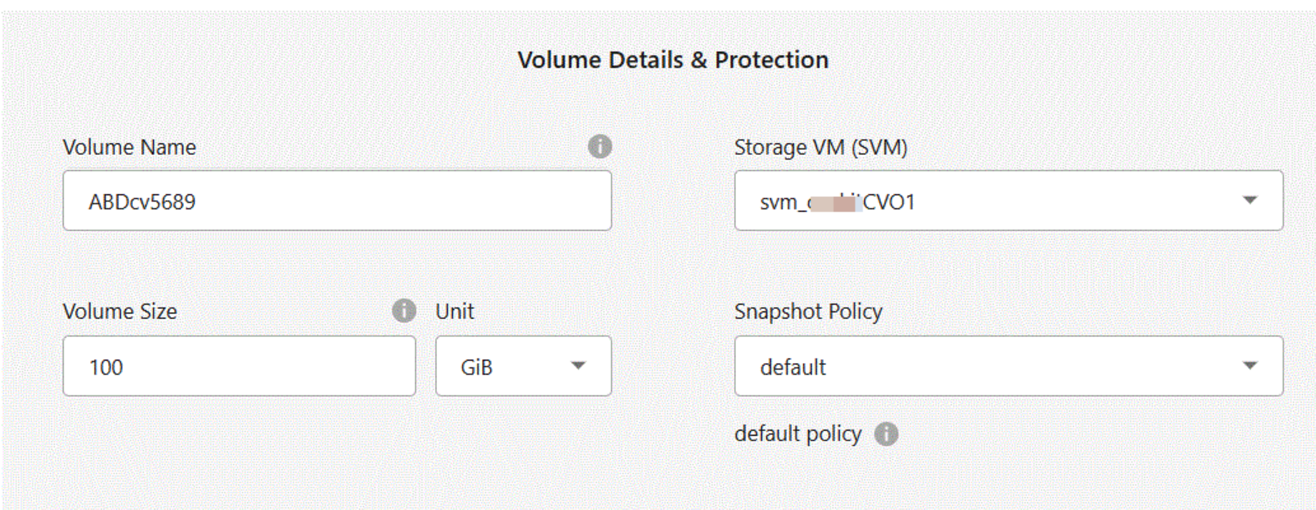
    Learn about supported client protocols and versions.

    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, the Console 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.

Field	Description
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, the Console 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 first page of the volume creation wizard:



15. **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. If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.
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 Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=Cloud** in this field. Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD
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. Refer to the NetApp Console 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.

16. **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, refer to Choose a volume usage profile, Data tiering overview, and KB: What Inline Storage Efficiency features are supported with CVO?

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

    a. Review details about the configuration.

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

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

    d. Click **Go**.

Result

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the **Audit** page.

If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the system 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 ONTAP System Manager or the ONTAP CLI.

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

> After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Google Cloud portal, such as the system tags, and the labels set in the Google Cloud resources. Any changes made to these configurations may lead to unexpected behavior or data loss.

Related links

- Planning your Cloud Volumes ONTAP configuration in Google Cloud

Google Cloud Platform Image Verification

Learn how Google Cloud image is verfied in Cloud Volumes ONTAP

Google Cloud image verification complies with enhanced NetApp security requirements. Changes have been made to the script generating the images to sign the image along the way using private keys specifically generated for this task. You can verify the integrity of the Google Cloud image by using the signed digest and public certificate for Google Cloud which can be downloaded via NSS for a specific release.

> Google Cloud image verification is supported on Cloud Volumes ONTAP software version 9.13.0 or greater.

Convert Google Cloud image to raw format for Cloud Volumes ONTAP

The image being used to deploy new instances, upgrades, or being used in existing images will be shared with the clients through the NetApp Support Site (NSS). The signed digest, and the certificates will be available to download through the NSS portal. Make sure you are downloading the digest and certificates for the right release corresponding to the image shared by NetApp Support. For instance, 9.13.0 images will have a 9.13.0 signed digest and certificates available on NSS.

Why is this step needed?

The images from Google Cloud cannot be downloaded directly. In order to verify the image against the signed digest and the certificates, you need to have a mechanism to compare the two files and download the image. To do so, you must export/convert the image into a disk.raw format and save the results in a storage bucket in Google Cloud. The disk.raw file is tarred and gzipped in the process.

The user/service-account will need privileges to perform the following:

- Access to Google storage bucket
- Write to Google Storage bucket
- Create cloud build jobs (used during export process)
- Access to the desired image
- Create export image tasks

To verify the image, it must be converted to a disk.raw format and then downloaded.

Use Google Cloud command line to export Google Cloud image

The preferred way to export an image to Cloud Storage is to use the gcloud compute images export command. This command takes the provided image and converts it to a disk.raw file which gets tarred and gzipped. The generated file is saved at the destination URL and can then be downloaded for verification.

The user/account must have privileges to access and write to the desired bucket, export the image, and cloud builds (used by Google to export the image) to execute this operation.

Export Google Cloud image using gcloud

Click to display

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

Extract zipped files

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

> For more information on how to export an image through Google Cloud, refer to the Google Cloud doc on Exporting an image.

Image signature verification

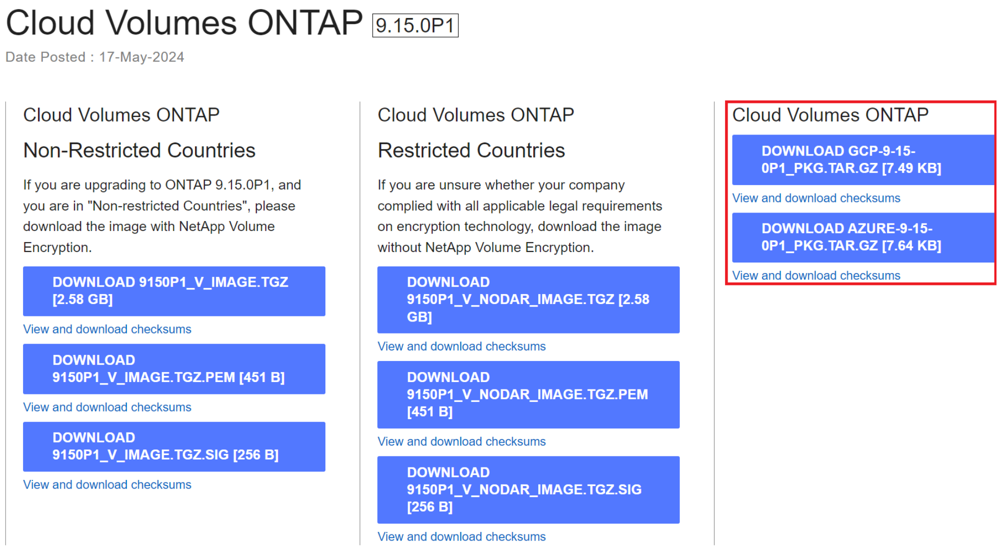
Google Cloud image signature verification for Cloud Volumes ONTAP

To verify the exported Google Cloud signed image, you must download the image digest file from the NSS to validate the disk.raw file and digest file contents.

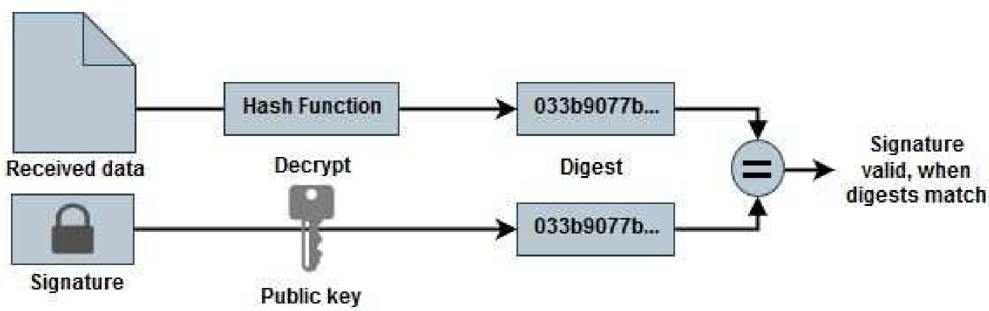
Signed image verification workflow summary

The following is an overview of the Google Cloud signed image verification workflow process.

- From the NSS, download the Google Cloud archive containing the following files:
  - Signed digest (.sig)
  - Certificate containing the public key (.pem)
  - Certificate chain (.pem)



- Download the converted disk.raw file
- Validate the certificate using the certificate chain
- Validate the signed digest using the certificate contain the public key
  - Decrypt the signed digest using the public key to extract the digest of the image file
  - Create a digest of the downloaded disk.raw file
  - Compare the two digest file for validation



Verify the Google Cloud image disk.raw file for Cloud Volumes ONTAP using OpenSSL

You can verify the Google Cloud downloaded disk.raw file against the digest file contents available through the NSS using OpenSSL.

> ⓘ The OpenSSL commands to validate the image are compatible with Linux, macOS, and Windows machines.

Steps

1. Verify the certificate using OpenSSL.

Click to display

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
        e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
        22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
        38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
        fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
        bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. Place the downloaded disk.raw file, the signature, and certificates in a directory.
3. Extract the public key from the certificate using OpenSSL.
4. Decrypt the signature using the extracted public key and verify the contents of the downloaded disk.raw file.

Click to display

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Use Cloud Volumes ONTAP

License management

Manage capacity-based licensing for Cloud Volumes ONTAP

Manage your capacity-based licenses from the NetApp Console 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.

You can manage capacity-based Cloud Volumes ONTAP licenses from the NetApp Console.

> While the actual usage and metering for the products and services managed in the Console are always calculated in GiB and TiB, the terms GB/GiB and TB/TiB are used interchangeably. This is reflected in the Cloud Marketplace listings, price quotes, listing descriptions, and in other supporting documentation

Learn more about Cloud Volumes ONTAP licenses.

How licenses are added to NetApp Console

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

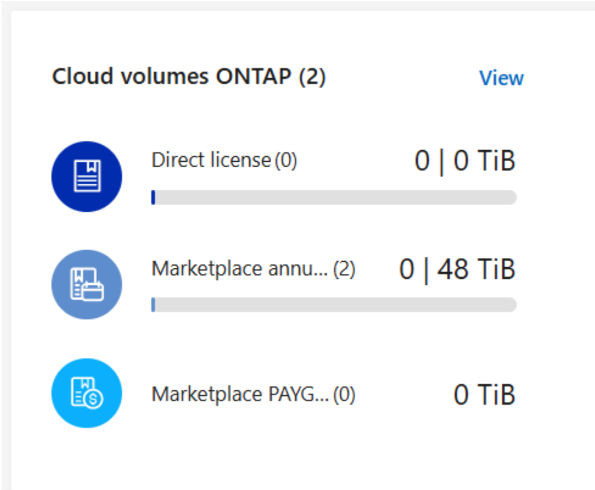
If the Console can't add the license, you'll need to manually add them. For example, if the Console agent is installed at a location that doesn't have internet access, you'll need to add the licenses yourself. Learn how to add purchased licenses to your account.

View the consumed capacity in your account

The Console 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 pane, select **Administration > Licenses and subscriptions**.
2. On the **Overview** tab, the Cloud Volumes ONTAP tile displays the current capacity provisioned for your account.



  - *Direct license* 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.
  - *Annual contract* is the total licensed capacity (bring your own license (BYOL) or Marketplace Contract) that you purchased from NetApp.
  - *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 Console.

3. Select **View** to see the consumed capacity for each of your licensing packages.
4. Select the **Licenses** tab to see details for each package license that you have purchased.

   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.

5. Select the **Subscriptions** tab to see the consumed capacity by license consumption model. This tab includes both PAYGO and annual contract licenses.

   You'll only see the subscriptions that are associated with the organization that you are that you're currently viewing.

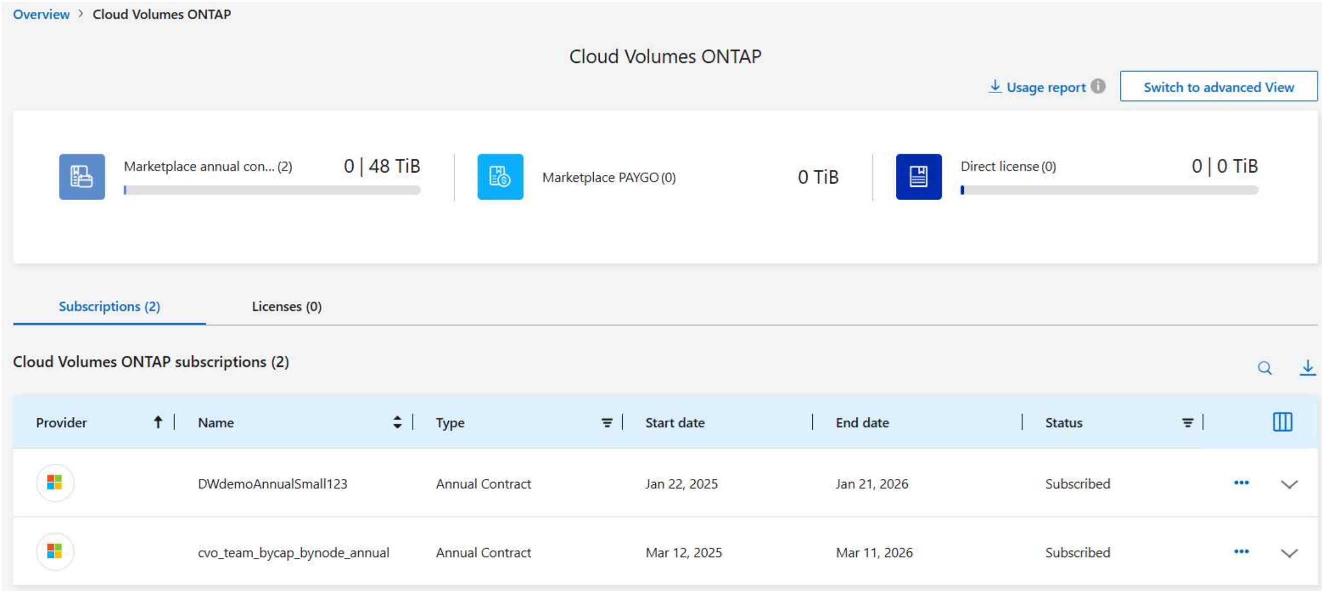
6. As you view the information about your subscriptions, you can interact with the details in the table. Expand a row to view more details.
   - Select to choose which columns appear in the table.
     Note that the Term and Auto Renew columns don't appear by default. The Auto Renew column displays renewal information for Azure contracts only.

Viewing package details

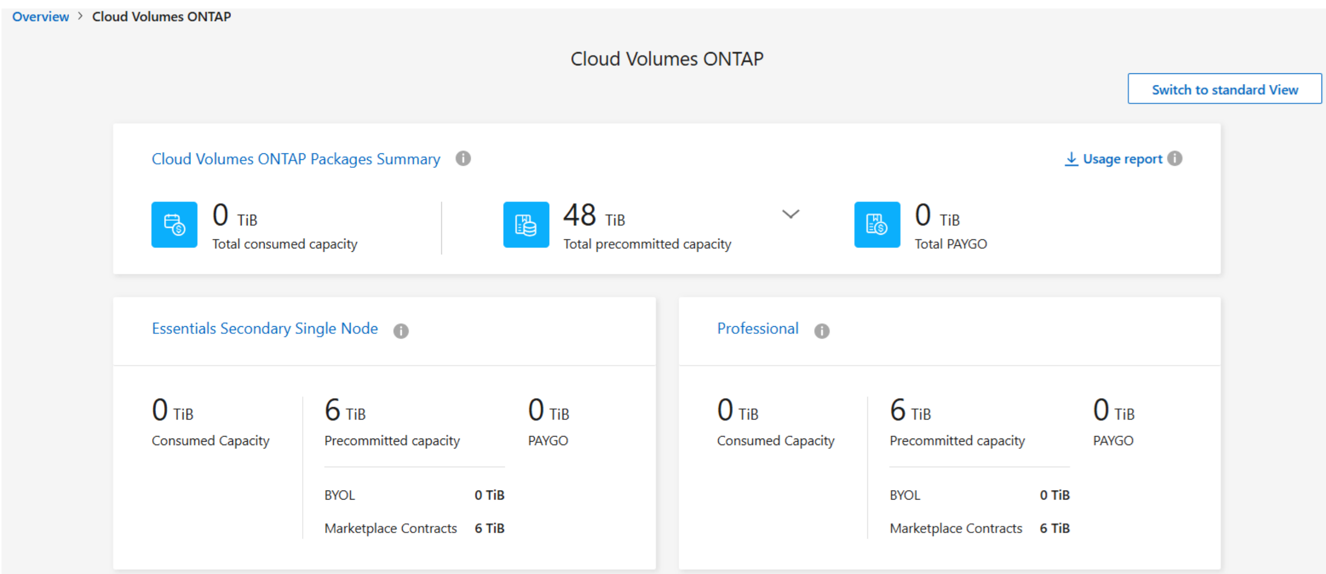
You can view details about the capacity used per package by switching to legacy mode on the Cloud Volumes ONTAP page.

1. From the left navigation pane, select **Administration > Licenses and subscriptions**.
2. On the **Overview** tab, the Cloud Volumes ONTAP tile displays the current capacity provisioned for your account.
3. Select **View** to see the provisioned capacity for each of your licensing packages.

4. Select **Switch to advanced view**.



5. View the details of the package you want to see.



Change charging methods

Capacity-based licensing is available in the form of a *package*. When you create a Cloud Volumes ONTAP system, you can choose from several licensing packages based on your business needs. If your needs change after you create the system, you can change the package at any time. For example, you might change from the Essentials package to the Professional package.

Learn more about capacity-based licensing packages.

About this task

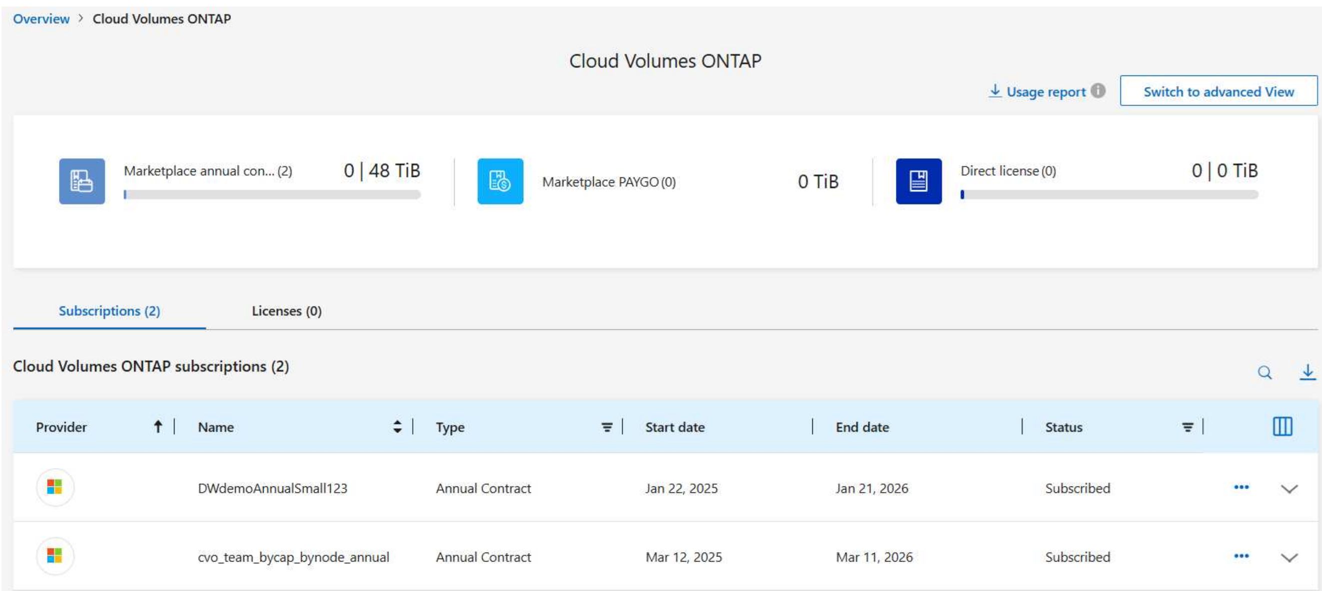
- Changing the charging method doesn't affect whether you're charged through a license purchased from NetApp (BYOL) or from your cloud provider's marketplace pay-as-you-go (PAYGO) subscription.

  The Console always attempts to charge against a license first. If a license isn't available, it charges against a marketplace subscription. You don’t have to convert a BYOL subscription to marketplace subscription or vice versa.

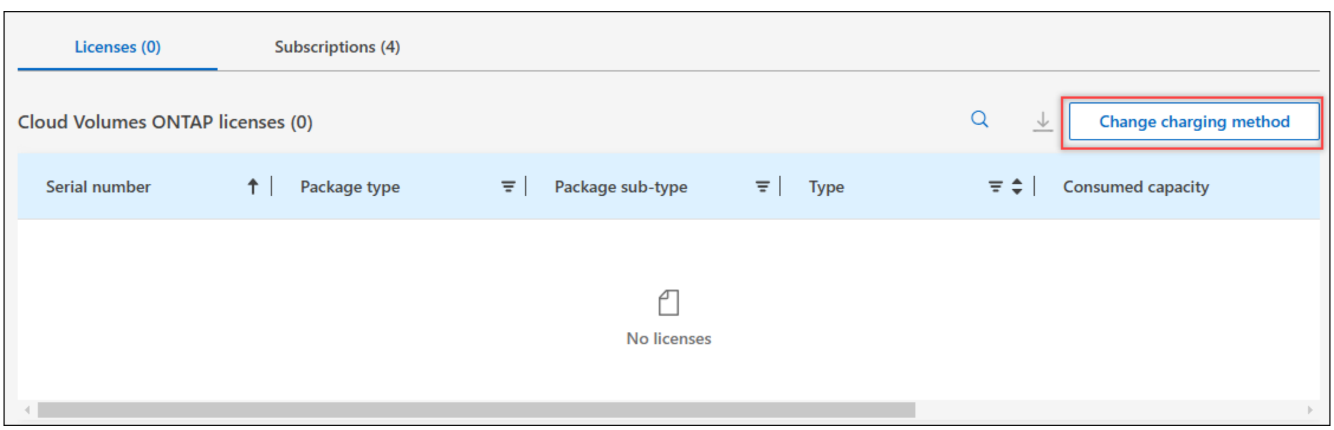
* If you have a private offer or contract from your cloud provider’s marketplace, changing to a charging method that’s not included in your contract will result in charging against BYOL (if you purchased a license from NetApp) or PAYGO.

Steps

1. From the left navigation pane, select **Administration > Licenses and subscriptions**.
2. Select the **Overview** tab.
3. On the Cloud Volumes ONTAP tile, select **View**.
4. Select **Switch to advanced view**.



5. Scroll down to the **Capacity-based license** table and select **Change charging method**.



6. On the **Change charging method** pop-up, select a Cloud Volumes ONTAP system, choose the new charging method, and then confirm your understanding that changing the package type will affect service charges.
7. Select **Change charging method**.

Download usage reports

You can download four usage reports from the Console. These usage reports provide capacity details of your subscriptions and tell you how you're being charged for the resources in your Cloud Volumes ONTAP subscriptions. The downloadable reports capture data at a point in time and can be easily shared with others.

The following reports are available for download. Capacity values shown are in TiB.

- **High-level usage**: This report includes the following information:
  - Total consumed capacity
  - Total precommitted capacity
  - Total BYOL capacity
  - Total Marketplace contracts capacity
  - Total PAYGO capacity
- **Cloud Volumes ONTAP package usage**: This report includes the following information for each package:
  - Total consumed capacity
  - Total precommitted capacity
  - Total BYOL capacity
  - Total Marketplace contracts capacity
  - Total PAYGO capacity
- **Storage VMs usage**: This report shows how charged capacity is broken down across Cloud Volumes ONTAP systems and storage virtual machines (SVMs). This information is only available in the report. It contains the following information:
  - System ID and name (appears as the UUID)
  - Cloud
  - NetApp account ID
  - System configuration
  - SVM name
  - Provisioned capacity
  - Charged capacity roundup
  - Marketplace billing term
  - Cloud Volumes ONTAP package or feature
  - Charging SaaS Marketplace subscription name
  - Charging SaaS Marketplace subscription ID
  - Workload type

- **Volumes usage**: This report shows how charged capacity is broken down by volumes in a Cloud Volumes ONTAP system. This information is not available on any screen in the Console. It includes the following information:
  - System ID and name (appears as the UUID)
  - SVN name
  - Volume ID
  - Volume type
  - Volume provisioned capacity

> FlexClone volumes aren't included in this report because these types of volumes don't incur charges.

Steps

1. From the left navigation pane, select **Administration > Licenses and subscriptions**.
2. On the **Overview** tab, select **View** from the Cloud Volumes ONTAP tile.
3. Select **Usage report**.

   The usage report downloads.

4. Open the downloaded file to access the reports.

Manage Keystone subscriptions for Cloud Volumes ONTAP through NetApp Console

Manage your Keystone subscriptions in the NetApp Console by enabling subscriptions for use with Cloud Volumes ONTAP and by requesting changes to the committed capacity for your subscription's service levels. Requesting additional capacity for a service level provides more storage for Cloud Volumes ONTAP systems.

NetApp Keystone is a flexible pay-as-you-grow subscription-based service that delivers a hybrid cloud experience for customers who prefer OpEx to CapEx or leasing.

Learn more about Keystone

Authorize your account

Before you can use and manage Keystone subscriptions in the Console, you need to contact NetApp to authorize your Console account with your Keystone subscriptions.

Steps

1. From the NetApp Console menu, select **Administration > Licenses and subscriptions**.
2. Select **Keystone Subscriptions**.
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 account to access the subscriptions.

4. Come back to the **Keystone Subscriptions** tab to view your subscriptions.

Link a subscription

After NetApp authorizes your account, you can link Keystone 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 NetApp Console menu, select **Administration > Licenses and subscriptions**.
2. Select **Keystone Subscriptions**.
3. For the subscription that you want to link, click ••• and select **Link**.

Result

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

Request more or less committed capacity

If you want to change the committed capacity for your subscription's service levels, you can send a request to NetApp directly from the Console. Requesting additional capacity for a service level provides more storage for Cloud Volumes ONTAP systems.

Steps

1. From the NetApp Console menu, select **Administration > Licenses and subscriptions**.
2. Select **Keystone Subscriptions**.
3. For the subscription that you want to 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.

Monitor usage

The Digital Advisor dashboard enables you to monitor Keystone subscription usage and generate reports.

Learn more about monitoring subscription usage

Unlink a subscription

If you no longer want to use a Keystone subscription with the Console, 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 NetApp Console menu, select **Administration > Licenses and subscriptions**.
2. Select **Keystone**.
3. For the subscription that you want to unlink, click ••• and select **Unlink**.

Result

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

Manage node-based licensing for Cloud Volumes ONTAP

Manage node-based licenses in the NetApp Console 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):

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

You can manage node-based Cloud Volumes ONTAP licenses licenses from the NetApp Console.

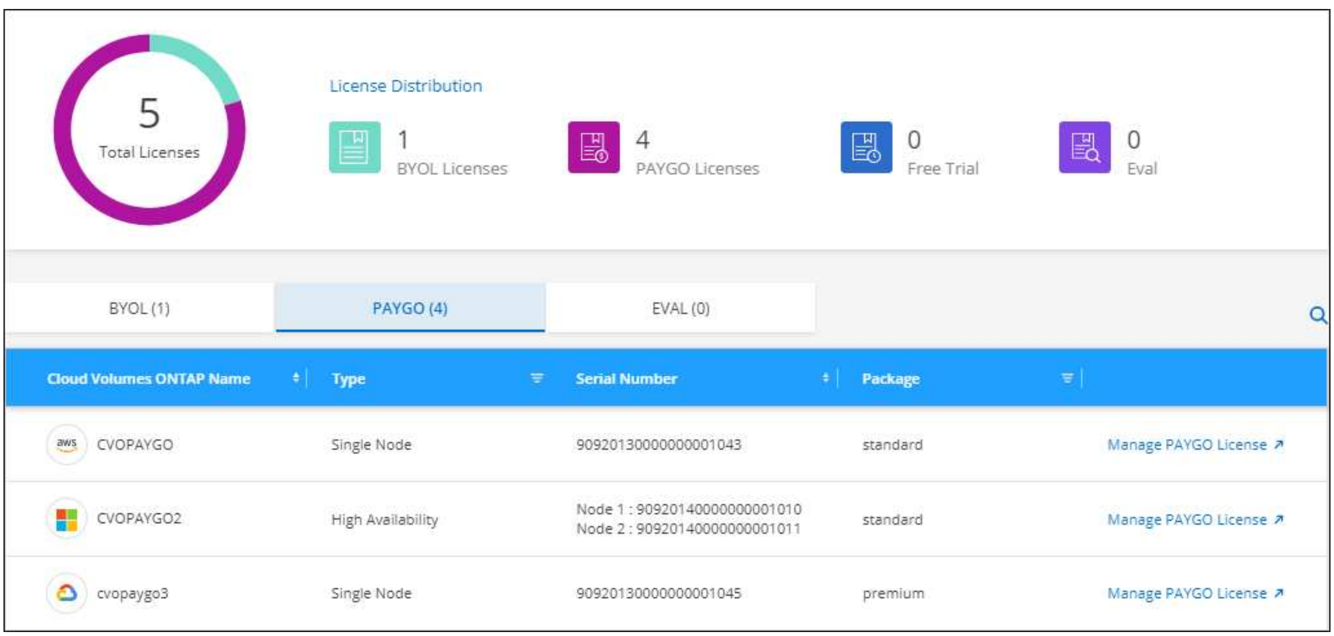
Learn more about Cloud Volumes ONTAP licenses.

Manage PAYGO licenses

The Licenses and subscriptions menu 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 pane, select **Administration > Licenses and subscriptions**.
2. Select the **Overview** tab.
3. On the Cloud Volumes ONTAP tile, select **View**.
4. Select **Node Based Licenses** from the drop-down.
5. Click **PAYGO**.
6. View details in the table about each of your PAYGO licenses.



7. 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.

> NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP.

Add unassigned licenses

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

Steps

1. From the left navigation pane, select **Administration > Licenses and subscriptions**.
2. Select the **Overview** tab.
3. On the Cloud Volumes ONTAP tile, select **View**.
4. Select **Node Based Licenses** from the drop-down.
5. Click **Unassigned**.
6. Click **Add Unassigned Licenses**.
7. 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.

8. Click **Add License**.

Result

The Console adds the license. 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 **Licenses and subscriptions**.

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 NetApp Backup and Recovery license, a NetApp Data Classification license, or a NetApp 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 direct license
- Licensing for a Cloud Volumes ONTAP single node is converted to a 32 TiB direct license

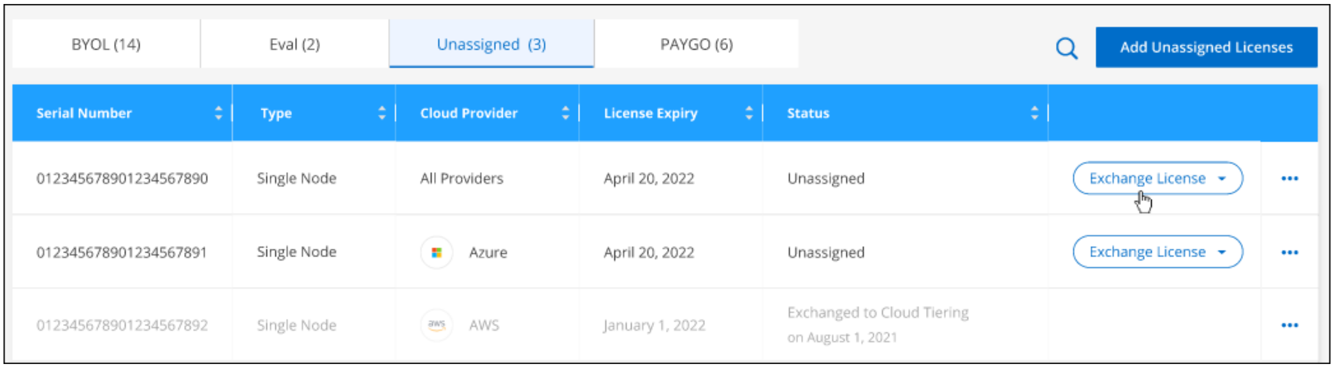
The converted license has the same expiration date as the Cloud Volumes ONTAP license.

View walkthrough of how to exchange node-based licenses.

Steps

1. From the left navigation pane, select **Administration > Licenses and subscriptions**.
2. Select the **Overview** tab.
3. On the Cloud Volumes ONTAP tile, select **View**.
4. Select **Node Based Licenses** from the drop-down.

5. Click **Unassigned**.
6. Click **Exchange License**.



7. Select the service that you'd like to exchange the license with.
8. If you're prompted, select an additional license for the HA pair.
9. Read the legal consent and click **Agree**.

Result

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

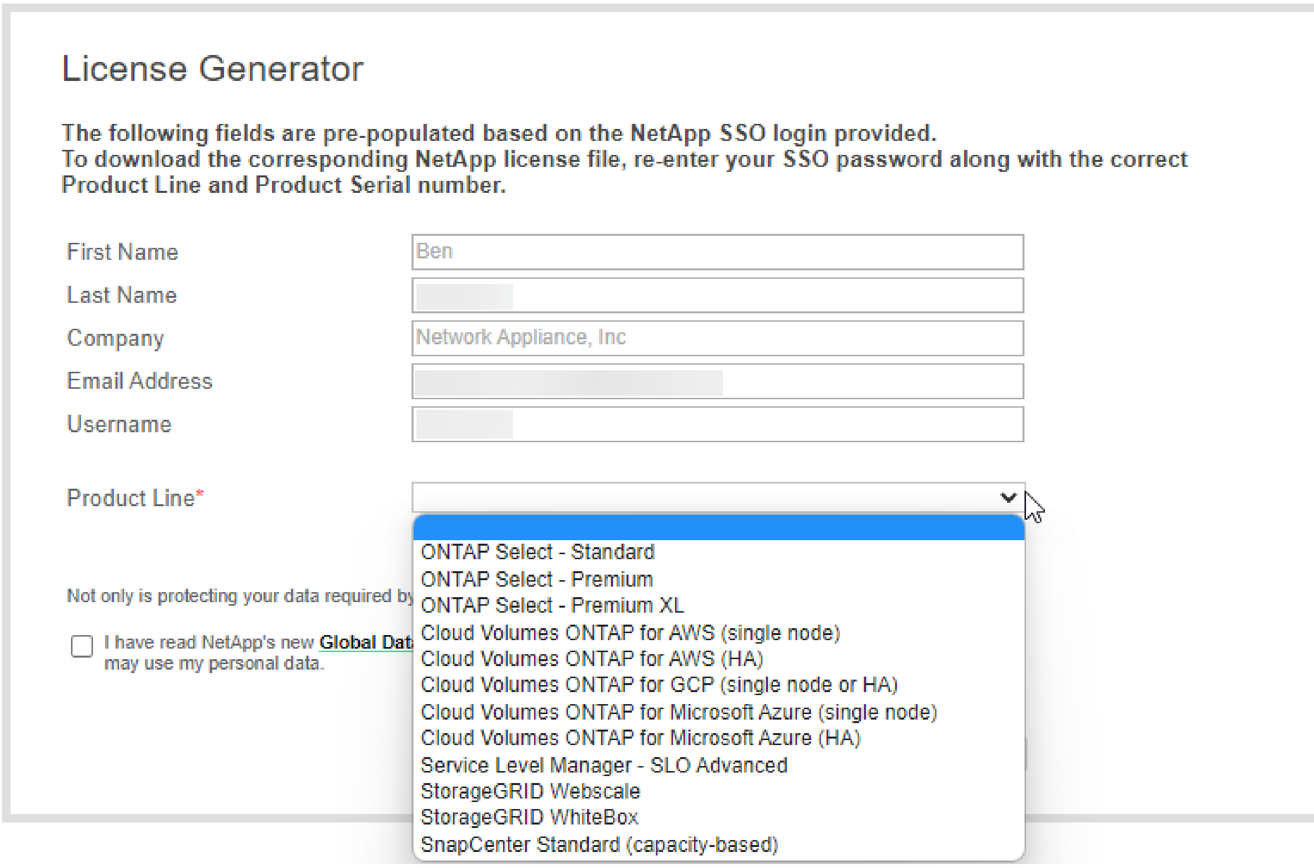
Obtain a system license file

In most cases, the Console 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, the Console automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system. If the Console can't access the license file over the secure internet connection, you can obtain the file yourself and then manually upload the file.

Steps

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

Result

The Console 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 the Console. After you purchase the license, you can apply it to a Cloud Volumes ONTAP system.

Steps

1. From the left navigation pane, select **Administration > Licenses and subscriptions**.
2. Select the **Overview** tab.
3. On the Cloud Volumes ONTAP tile, select **View**.
4. Select **Node Based Licenses** from the drop-down.
5. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
6. Click **Add Capacity License**.
7. Enter the serial number or upload the license file (or files if you have an HA pair).
8. 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 the Console.

Steps

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

4. Select **Node Based Licenses** from the drop-down.
5. In the **BYOL** tab, expand the details for a Cloud Volumes ONTAP system.
6. Click the action menu next to the capacity license and select **Remove License**.
7. Click **Remove**.

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 system.
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 system.

   Learn how to delete a Cloud Volumes ONTAP system.

Related links

<a href="https://docs.netapp.com/us-en/storage-management-cloud-volumes-ontap/End of availability of node-based licenses
 xref:./task-convert-node-capacity.html">Convert node-based licenses to capacity based

Volume and LUN administration

Create a FlexVol volume on a Cloud Volumes ONTAP system

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 the NetApp Console.

You have several ways to create a new volume:

- Specify details for a new volume and let the Console handle the underlying data aggregates for you. Learn more
- Create a volume on a data aggregate of your choice. Learn more
- Create a volume on the second node in an HA configuration. Learn more

Before you begin

A few notes about volume provisioning:

- When you create an iSCSI volume, the Console 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 ONTAP System Manager or the ONTAP CLI.

- If you want to use CIFS in AWS, you must have set up DNS and Active Directory. For details, refer to Networking requirements for Cloud Volumes ONTAP for AWS.
- If your Cloud Volumes ONTAP configuration supports the Amazon EBS Elastic Volumes feature, you might want to learn more about what happens when you create a volume.

Create a volume

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

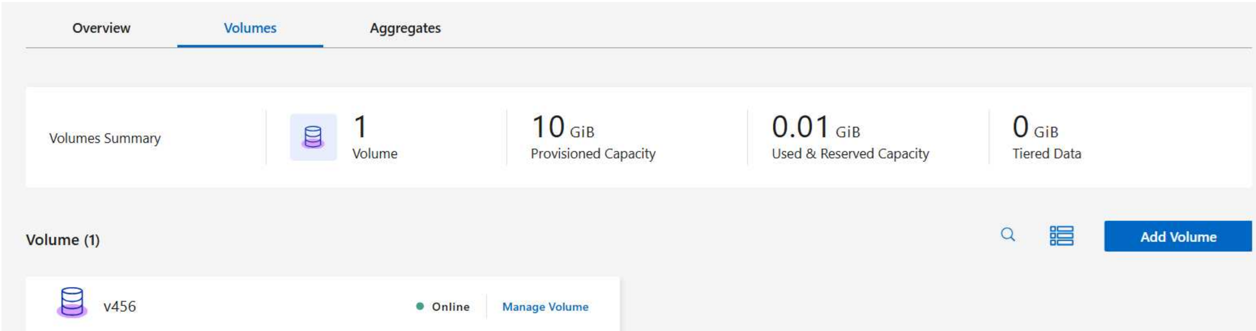
Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, double-click the name of the Cloud Volumes ONTAP system on which you want to provision a FlexVol volume.

   You can create a volume by letting the Console 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.

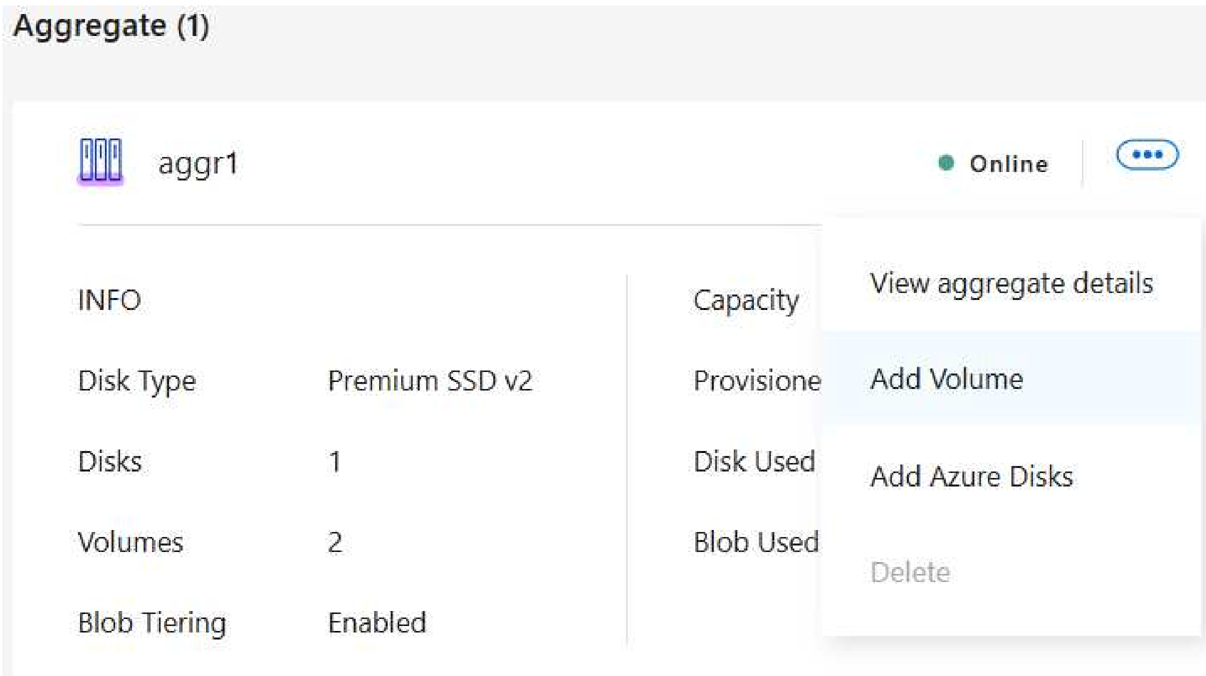
Any aggregate

Select the Volumes tab, and click **Add Volume**.



Specific aggregate

1. On the **Aggregates** tab, go to the required the aggregate and click the ••• icon.
2. Select **Add 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 Name	The identifiable name you can enter for the new volume.
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.

Field	Description
Storage VM (SVM)	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. You can specify the Storage VM for the new volume.
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, the Console 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, the Console 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.

If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.

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 AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=corp** in this field.
- 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
- To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=Cloud** in this field.
  Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD

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. For information, refer to the NetApp Console automation docs.

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, the Console 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 AWS
   - Sizing your system in Azure
   - Sizing your system in Google Cloud

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

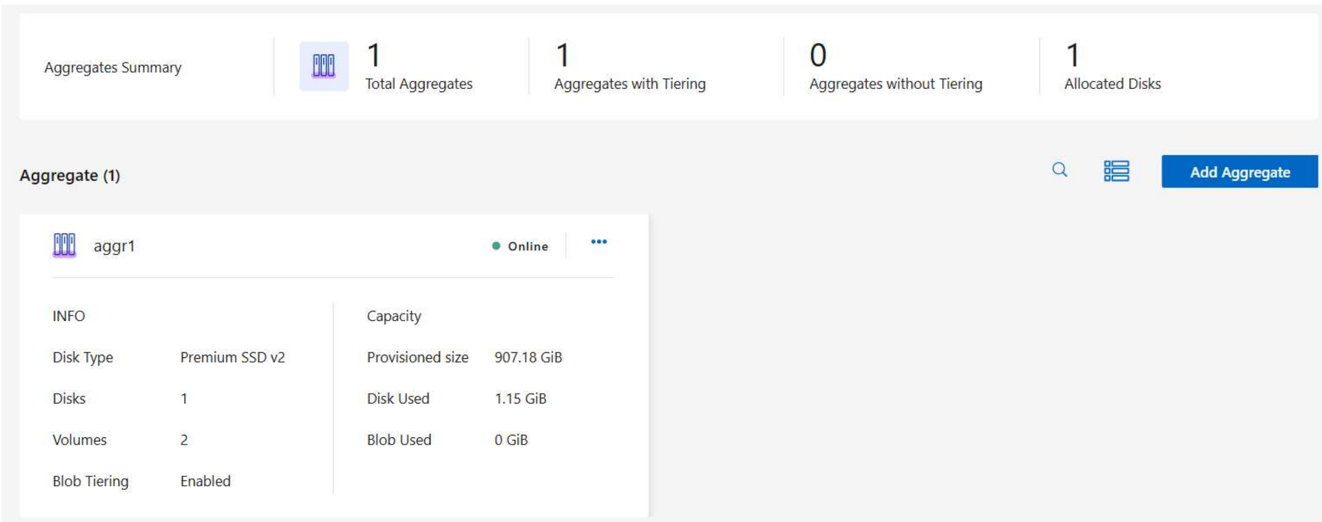
The Console creates the volume on the Cloud Volumes ONTAP system.

Create a volume on the second node in an HA configuration

By default, the Console 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. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, double-click the name of the Cloud Volumes ONTAP system on which you want to manage aggregates.
3. On the Aggregates tab, click **Add Aggregate**, and create the aggregate.



4. For Home Node, choose the second node in the HA pair.
5. After the Console creates the aggregate, select it and then click **Create volume**.
6. Enter details for the new volume, and then click **Create**.

Result

The Console creates the volume on the second node in the HA pair.

For HA pairs deployed in multiple AWS Availability Zones, you must mount the volume to clients by using the floating IP address of the node on which the volume resides.

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

Manage volumes on Cloud Volumes ONTAP systems

You can manage volumes and CIFS servers in the NetApp Console. You can also move volumes to avoid capacity issues.

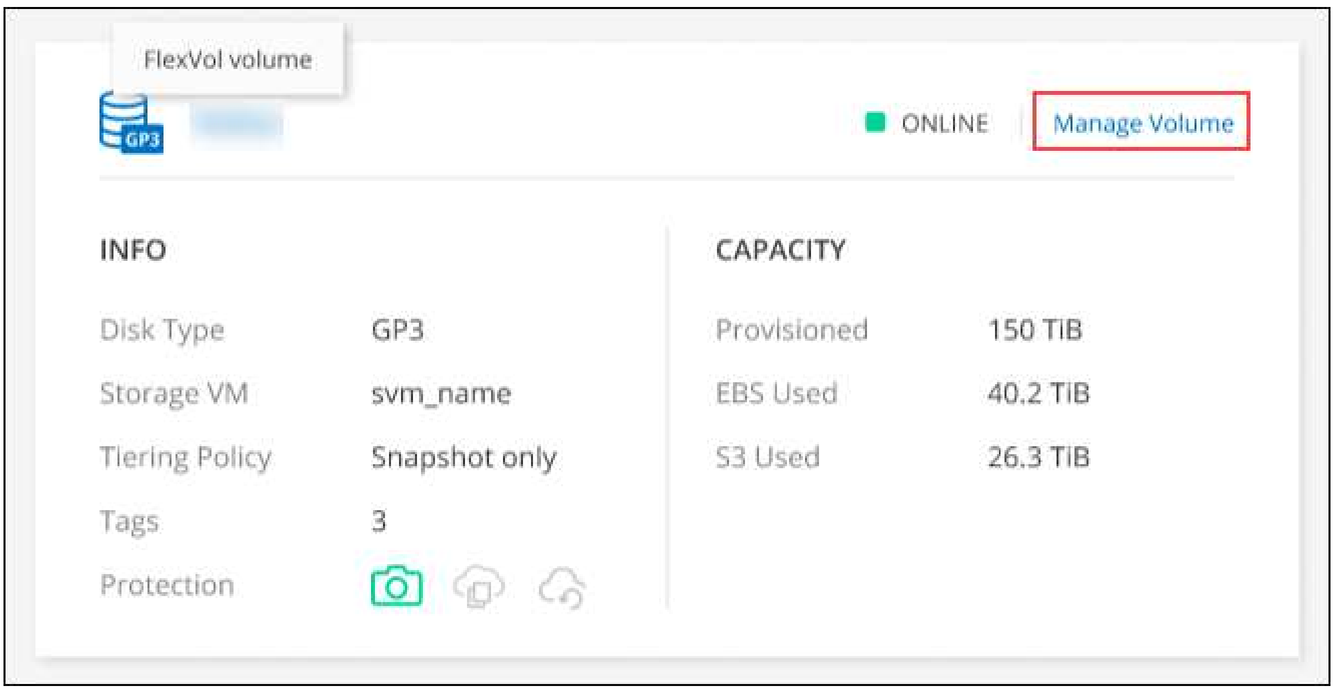
You can manage volumes in the NetApp Console Standard View or through ONTAP System Manager that is included within the Console for advanced volume management. The Standard View provides a limited set of options to modify your volumes. System Manager provides advanced level of management, such as cloning, resizing, changing settings for anti-ransomware, analytics, protection, and activity tracking, and moving volumes across tiers. For information, refer to Administer Cloud Volumes ONTAP using System Manager.

Manage volumes

By using the Standard View of the Console, you can manage volumes according to your storage needs. You can view, edit, clone, restore, and delete volumes.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, double-click the Cloud Volumes ONTAP system on which you want to manage volumes.
3. Select the **Volumes** tab.



4. On the required volume tile, click **Manage volume**.

Task	Action
View information about a volume	Under Volume Actions in the Manage volumes panel, click **View volume details**.

<table>
<tr><th>Task</th><th>Action</th></tr>
<tr><td>Get the NFS mount command</td><td>a. Under Volume Actions in the Manage volumes panel, click Mount Command.
b. Click Copy.</td></tr>
<tr><td>Clone a volume</td><td>a. Under Volume Actions in the Manage volumes panel, click Clone the volume.
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, refer to the ONTAP 9 Logical Storage Management Guide.</td></tr>
<tr><td>Edit a volume (read-write volumes only)</td><td>a. Under Volume Actions in the Manage volumes panel, click Edit volume settings
b. Modify the volume’s Snapshot policy, NFS protocol version, NFS access control list (export policy), or share permissions, and then click Apply.

If you need custom Snapshot policies, you can create them by using ONTAP System Manager.</td></tr>
<tr><td>Delete a volume</td><td>a. Under Volume Actions in the Manage volumes panel, click Delete the volume.
b. Under the Delete Volume window, enter the name of the volume you want to delete.
c. Click Delete again to confirm.</td></tr>
<tr><td>Create a Snapshot copy on demand</td><td>a. Under Protection Actions in the Manage Volumes panel, click Create a Snapshot copy.
b. Change the name, if needed, and then click Create.</td></tr>
<tr><td>Restore data from a Snapshot copy to a new volume</td><td>a. Under Protection Actions in the Manage Volumes panel, click Restore from Snapshot copy.
b. Select a Snapshot copy, enter a name for the new volume, and then click Restore.</td></tr>
</table>

Task	Action
Change the underlying disk type	a. Under Advanced Actions in the Manage Volumes panel, click **Change Disk Type**. b. Select the disk type, and then click **Change**. The Console 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. Under Advanced Actions in the Manage Volumes panel, click **Change Tiering Policy**. b. Select a different policy and click **Change**. The Console 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. Type the name of the volume in the dialog. c. Click **Delete** again to confirm.

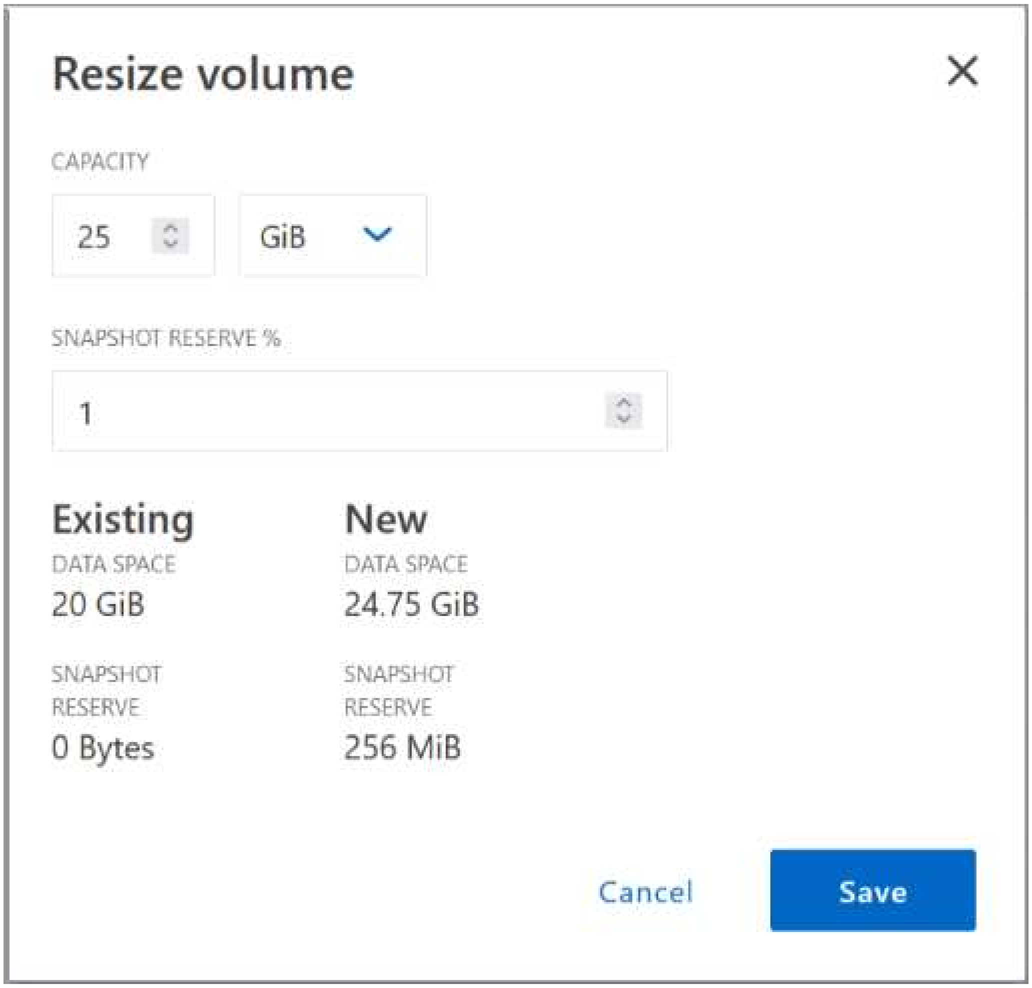
Resize a volume

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 its size. This value is configurable in the Console agent's settings.

If you need to resize your volume, you can do it from ONTAP System Manager in the Console.

Steps

1. Click the System Manager view to resize a volume through ONTAP System Manager. Refer to How to get started.
2. From the left navigation menu, select **Storage > Volumes**.
3. From the list of volumes, identify the one that you should resize.
4. Click the options icon .
5. Select **Resize**.
6. On the **Resize Volume** screen, edit the capacity and Snapshot reserve percentage as required. You can compare the existing, available space with the modified capacity.
7. Click **Save**.



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 information.

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 **Overview** tab of the Cloud Volumes ONTAP system, click the **Feature** tab under the right-side panel.
2. Under the CIFS Setup field, click the **pencil icon** to display the CIFS Setup window.
3. Specify settings for the CIFS server:

Task	Action
Select Storage VM (SVM)	Selecting the Cloud Volume ONTAP storage virtual machine (SVM) displays it's configured CIFS information.
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.

Task	Action
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.
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. If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.
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.
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 AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=corp** in this field. • 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 • To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=Cloud** in this field. Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD

4. Click **Set**.

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 ONTAP 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 ONTAP System Manager or the ONTAP CLI to move the volumes to the aggregate.

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

For instructions, refer to the ONTAP 9 Volume Move Express Guide.

Move a volume when Console displays an Action Required message

The Console 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.

> The Console 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 capacity issues.
2. Based on your analysis, move volumes to avoid capacity issues:
   - Move volumes to another system to avoid capacity issues.
   - Move volumes to another aggregate to avoid capacity issues.

Identify how to correct capacity issues

If the Console 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.

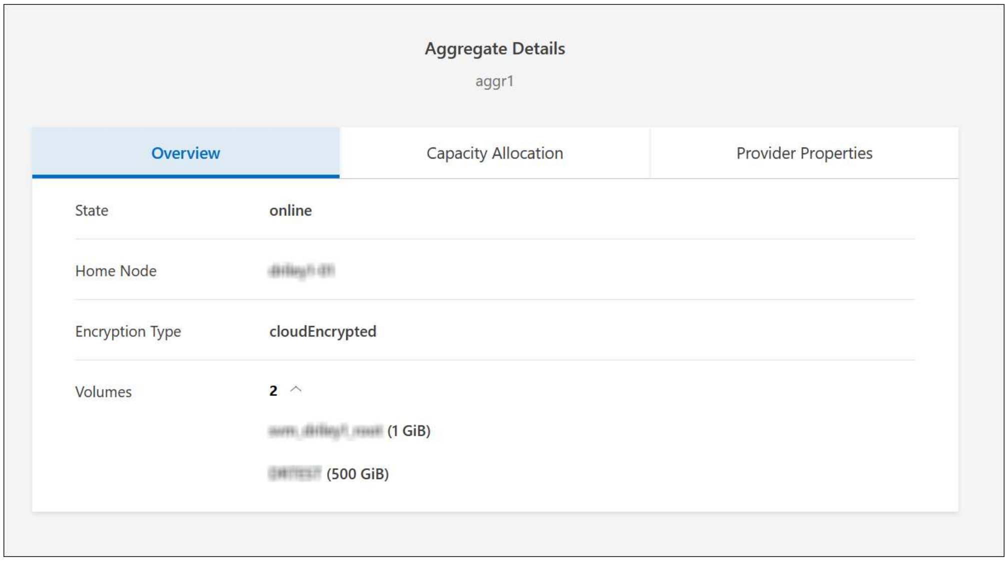
Steps

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 Cloud Volumes ONTAP system, click the **Aggregates tab**.
   b. On the aggregate tile, click the ••• icon and then click **View aggregate details**.
   c. Under the **Overview** tab of the **Aggregate Details** screen, 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 information, refer to Move 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 information, refer to Move volumes to another aggregate to avoid capacity issues.

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

      For information, refer to Move volumes to another aggregate 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, the Console 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 system to the target system to perform a one-time data replication of the volume.

   For information, refer to 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 information, refer to Managing data replication schedules and relationships.

4. Configure the volume for data access.

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

5. Delete the original volume.

   For information, refer to 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.

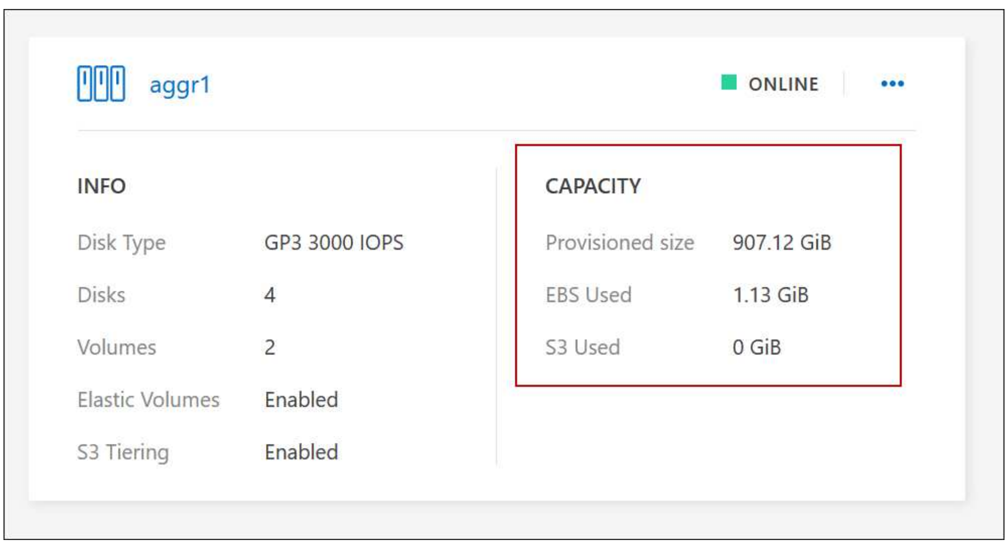
About this task

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, the Console 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. On Cloud Volumes ONTAP system, click the **Aggregates tab**.
   b. On the required aggregate tile, click the ••• icon and then **View aggregate details** to view the available capacity (provisioned size minus used aggregate capacity).



2. If needed, add disks to an existing aggregate:
   a. Select the aggregate, then click the ••• icon > **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 information, refer to Creating aggregates.

4. Use ONTAP System Manager or the ONTAP CLI to move the volumes to the aggregate.
5. In most situations, you can use System Manager to move volumes.

   For instructions, refer to the ONTAP 9 Volume Move Express Guide.

Reasons why a volume move might perform slowly

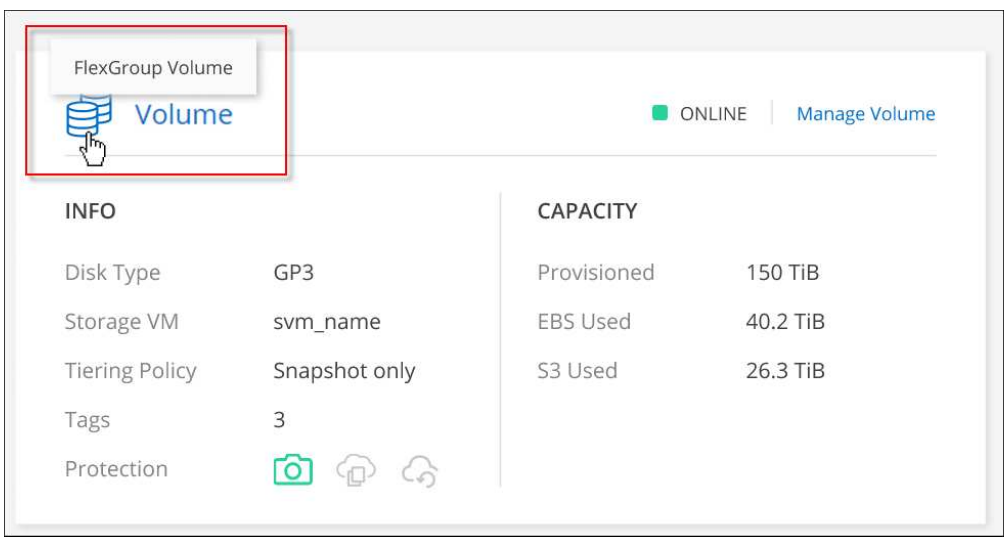
Moving a volume might take longer than you expect if any of the following conditions are true for Cloud Volumes ONTAP:

- 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.

View FlexGroup Volumes

You can view FlexGroup volumes created through ONTAP System Manager or the ONTAP CLI directly through the Volumes tab in the Console. You can see detailed information for the FleGroup volumes through a dedicated **Volumes** tile, where you can identify each FlexGroup volume group through the icon's hover text. Additionally, you can identify and sort FlexGroup volumes under the volumes list view through the Volume Style column.



> ℹ️ Currently, you can only view existing FlexGroup volumes under the Console. You can't create FlexGroup volumes in the Console.

Tier inactive Cloud Volumes ONTAP data to a 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, refer to 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 are good to go. Learn more.

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

- For AWS, you'll need a VPC Endpoint to Amazon Simple Storage Service (Amazon S3). Learn more.
- For Azure, you won't need to do anything as long as the NetApp Console has the required permissions. Learn more.
- For Google Cloud, you need to configure the subnet for Private Google Access and set up a service account. Learn more.

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

Data tiering should be enabled on an aggregate to enable it 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**

The NetApp Console prompts you to choose a tiering policy when you create, modify, or replicate a volume.

- Tier data from read-write volumes
- Tier data from 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. The Console does that for you.
- You don't need to enable data tiering at the system level.

  The Console creates an object store for cold data when it creates the system, 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 AWS

- Data tiering is supported in AWS beginning with Cloud Volumes ONTAP 9.2.
- The performance tier can be General Purpose SSDs (gp3 or gp2) or Provisioned IOPS SSDs (io1).

> We do not recommend tiering data to object storage when using Throughput Optimized HDDs (st1).

- The inactive data is tiered to Amazon S3 buckets. Tiering to other providers is not supported.

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.
- The inactive data is tiered to Microsoft Azure Blob. Tiering to other providers is not supported.

Support in Google Cloud

- Data tiering is supported in Google Cloud beginning with Cloud Volumes ONTAP 9.6.
- The performance tier can be either SSD persistent disks, balanced persistent disks, or standard persistent disks.
- The inactive data is tiered to Google Cloud Storage. Tiering to other providers is not supported.

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 Amazon S3

Ensure that Cloud Volumes ONTAP has a connection to Amazon S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, refer to the AWS Documentation: Creating a Gateway Endpoint.

When you create the VPC Endpoint, be sure to select the region, VPC, and route table that corresponds to the Cloud Volumes ONTAP instance. You must also modify the security group to add an outbound HTTPS rule that enables traffic to the S3 endpoint. Otherwise, Cloud Volumes ONTAP cannot connect to the S3 service.

If you experience any issues, refer to AWS Support Knowledge Center: Why can’t I connect to an S3 bucket using a gateway VPC endpoint?.

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 the Console has the required permissions. The Console enables a VNet service endpoint for you if the custom role for the Console agent has these permissions:

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

The custom role includes the permissions by default. View Azure permission for the Console agent

Requirements to tier cold data to a Google Cloud Storage bucket

- The subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access. For instructions, refer to Google Cloud Documentation: Configuring Private Google Access.
- A service account must be attached to Cloud Volumes ONTAP.

  Learn how to set up this service account.

  You're prompted to select this service account when you create a Cloud Volumes ONTAP system.

  If you don't select a service account during deployment, you'll need to shut down Cloud Volumes ONTAP, go to the Google Cloud Console, and then attach the service account to the Cloud Volumes ONTAP instances. You can then enable data tiering as described in the next section.

- To encrypt the bucket with customer-managed encryption keys, enable the Google Cloud storage bucket to use the key.

  Learn how to use customer-managed encryption keys with Cloud Volumes ONTAP.

Enable data tiering after implementing the requirements

The Console 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 through the API or ONTAP System Manager, which creates the object store.

> ⓘ The ability to enable tiering through the Console will be available in a future Cloud Volumes ONTAP release.

Ensure 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**

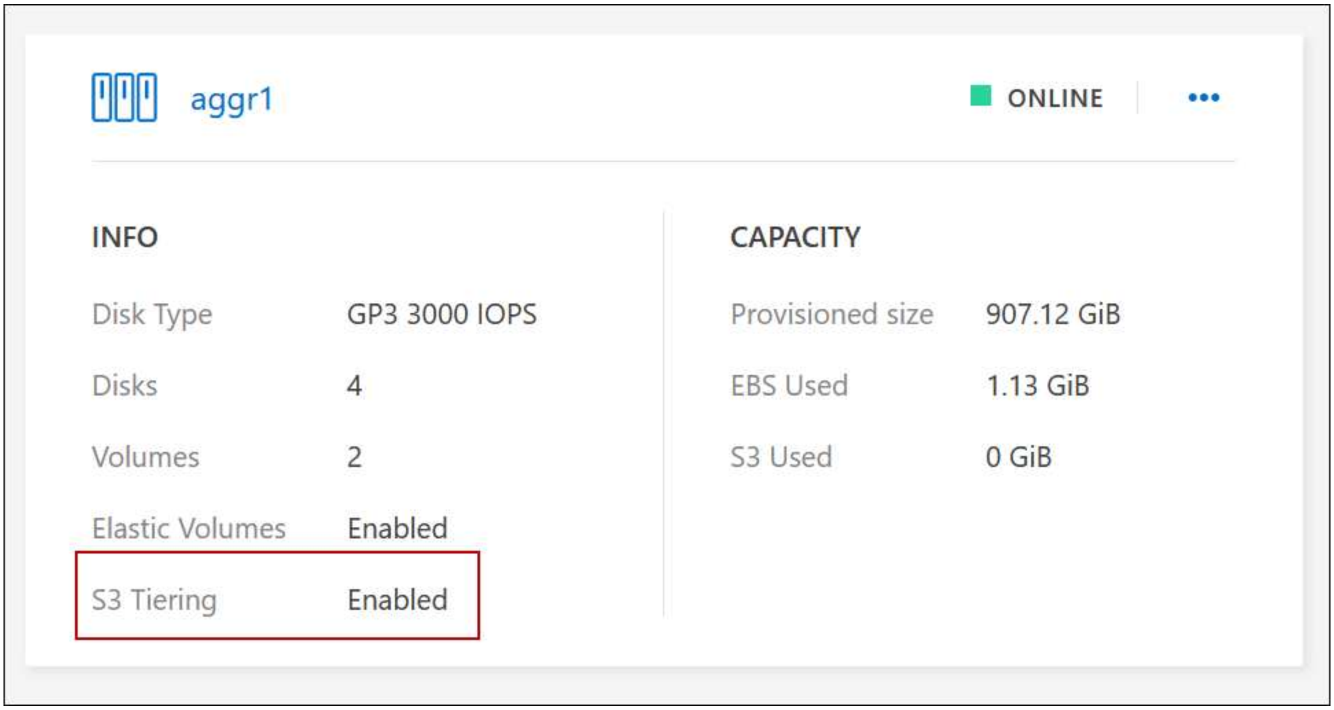
  If you're enabling data tiering on a new volume, then you don't need to worry about enabling data tiering on an aggregate. The Console creates the volume on an existing aggregate that has tiering enabled, or it creates a new aggregate for the volume if a data tiering-enabled aggregate doesn't already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

- **Existing volumes**

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

Steps to confirm whether tiering is enabled on an aggregate

1. From the left navigation menu, select **Storage > Management**.
2. Open the Cloud Volumes ONTAP system.
3. Select select the **Aggregates** tab and check if tiering is enabled or disabled on the aggregate.



Steps to enable tiering on an aggregate

1. In ONTAP 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.

Tier 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 **Volumes** tab under the system, create a new volume or change the tier of an existing volume:

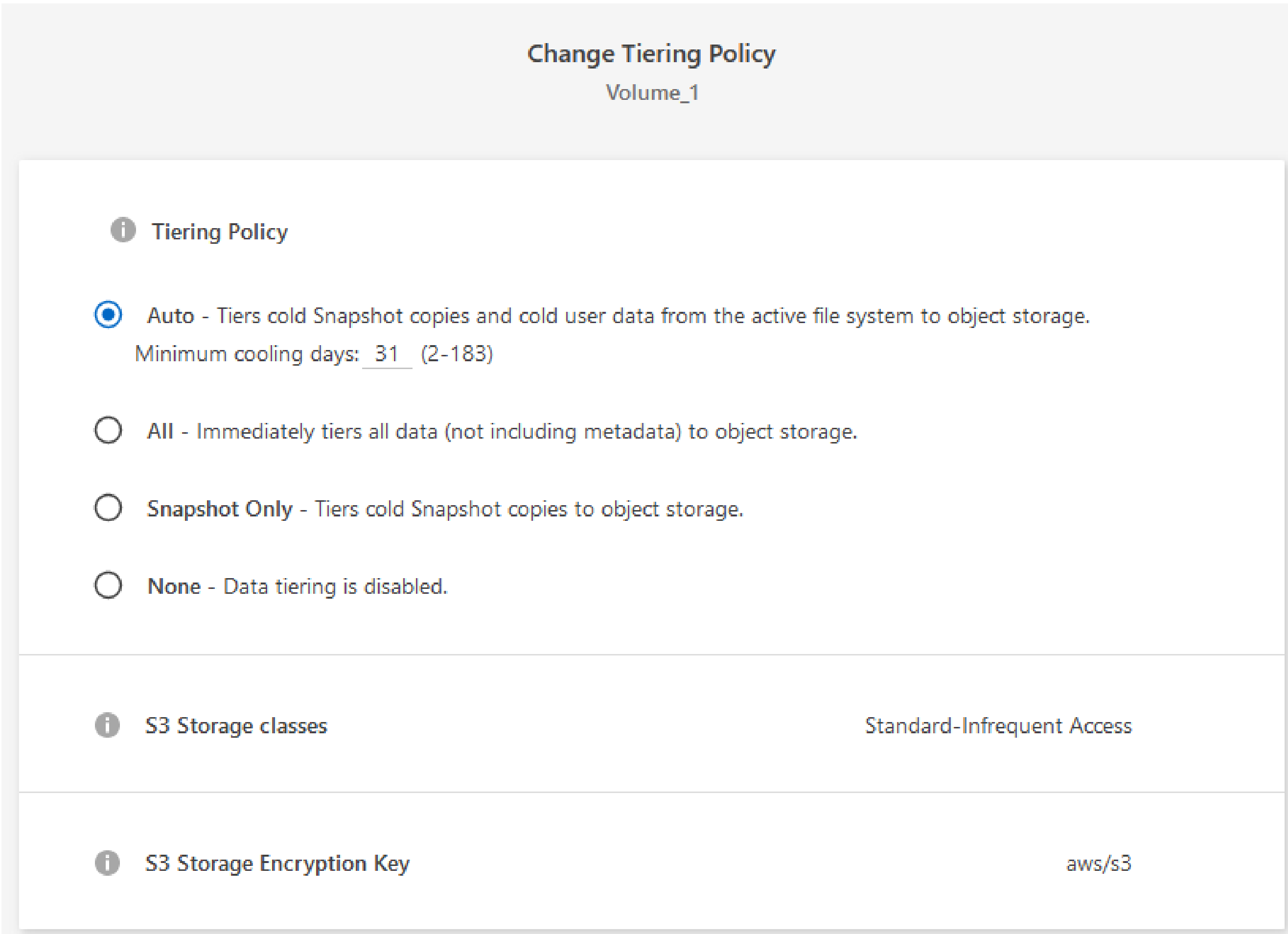
Task	Action
Create a new volume	Click **Add New Volume**.

Task	Action
Modify an existing volume	Select the desired volume tile, click **Manage volume** to access the Manage Volumes right-side panel, and then click **Advanced actions** and **Change tiering policy** under the right panel.

2. Select a tiering policy.

   For a description of these policies, refer to Data tiering overview.

   Example

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

Tier data from data protection volumes

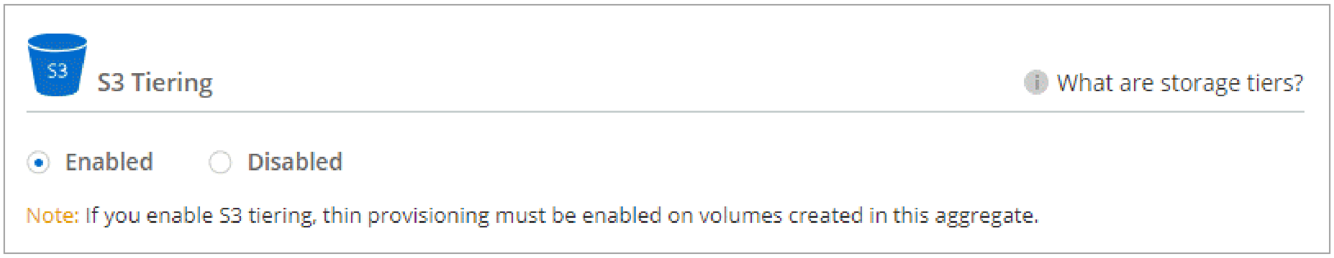
Cloud Volumes ONTAP can tier data from a data protection volume to a capacity tier. If you activate the destination volume, the data gradually moves to the performance tier as it is read.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, select the Cloud Volumes ONTAP system that contains the source volume, and then drag it to the system to which you want to replicate the volume.

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

   Example

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

Change 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, refer to Data tiering overview.

Steps

1. On the Cloud Volumes ONTAP system, click the menu icon and then click **Storage Classes** or **Blob Storage Tiering**.
2. Choose a storage class and then click **Save**.

Change 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. The Console can then purchase additional disks for you when additional capacity is required (up until you reach the disk limit for the aggregate).

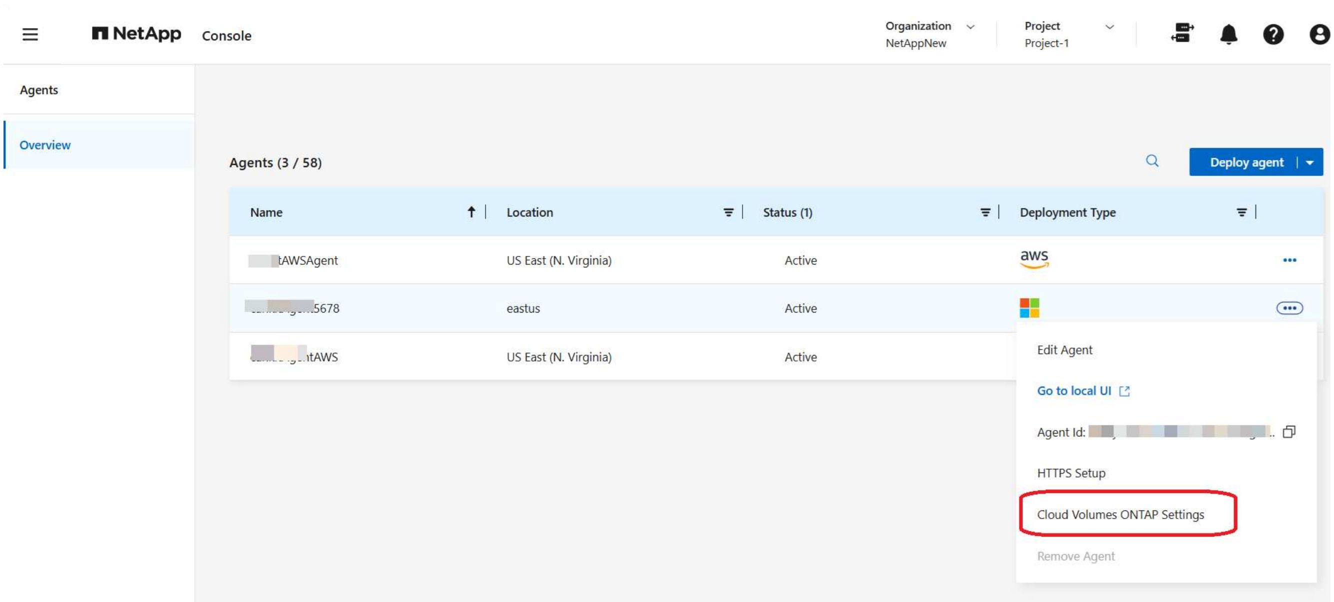
> If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data and you might experience performance degradation. Any change should be done with caution. If you're unsure, reach out to NetApp Support for guidance.

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.

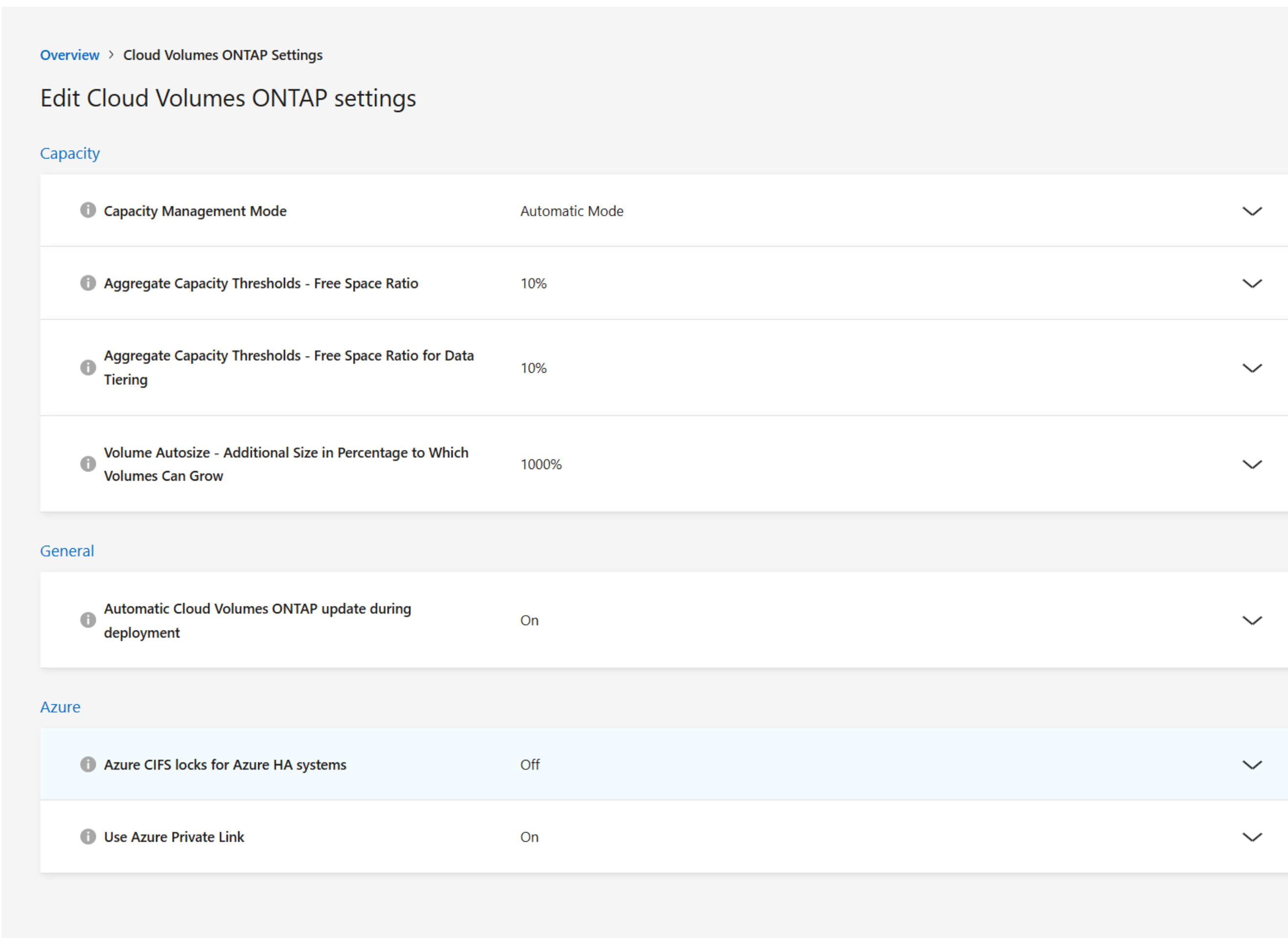
Steps

1. From the left navigation pane, go to **Administration > Agents**.
2. Click the ••• icon for the Console agent that manages your Cloud Volumes ONTAP system.

3. Select **Cloud Volumes ONTAP Settings**.



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



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

Change 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 ONTAP CLI and 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.

Remove an S3 bucket on decommissioning a system

You can delete an S3 bucket with the data tiered from a Cloud Volumes ONTAP system when you decommission the environment.

You can delete the S3 bucket only if:

- The Cloud Volume ONTAP system is deleted from the Console.
- All objects are deleted from the bucket and the S3 bucket is empty.

When you decommission a Cloud Volumes ONTAP system, the S3 bucket that was created for the environment is not deleted automatically. Instead, it remains in an orphaned state to prevent any accidental data loss. You can delete the objects in the bucket, then remove the S3 bucket itself, or keep it for later use. Refer to ONTAP CLI: vserver object-store-server bucket delete.

Connect to a LUN on Cloud Volumes ONTAP from your host system

When you create an iSCSI volume, the NetApp Console 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:

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

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, double-click the Cloud Volumes ONTAP system on which you want to manage volumes.
3. In the system, select the **Volumes** tab.
4. Go to the required volume tile and then select **Manage volume** to access the Manage Volumes panel on

the right.

5. Click **Target iQN**.
6. Click **Copy** to copy the iQN name.
7. 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 on a Cloud Volumes ONTAP system

A FlexCache volume is a storage volume that caches SMB and 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.

NetApp Console provides management of FlexCache volumes with the NetApp Volume Caching.

You can also 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

Work with FlexCache when the origin is encrypted

When configuring FlexCache on a Cloud Volumes ONTAP system where the origin volume is encrypted, additional steps are required, to ensure that the FlexCache volume can properly access and cache the encrypted data.

Before you begin

1. **Encryption setup**: Ensure that the source volume is fully encrypted and operational. For Cloud Volumes ONTAP systems, this involves integrating with cloud-specific key management services.
   For AWS, this typically means using AWS Key Management Service (KMS). For information, refer to Manage keys with AWS Key Management Service.
   For Azure, you need to set up Azure Key Vault for NetApp Volume Encryption (NVE). For information, refer to Manage keys with Azure Key Vault.
   For Google Cloud, it is Google Cloud Key Management Service. For information, refer to Manage keys with Google's Cloud Key Management Service.
2. **Key management services**: Before creating a FlexCache volume, verify that the key management services are configured correctly on the Cloud Volumes ONTAP system. This configuration is essential for the FlexCache volume to decrypt the data from the origin volume.
3. **Licensing**: Confirm that a valid FlexCache license is available and activated on the Cloud Volumes ONTAP system.
4. **ONTAP version**: Ensure that the ONTAP version of your Cloud Volumes ONTAP system supports FlexCache with encrypted volumes. Refer to the latest ONTAP release notes or compatibility matrix for more information.
5. **Network Configuration**: Ensure that the network configuration allows for seamless communication between the origin volume and the FlexCache volume. This includes proper routing and DNS resolution in a cloud environment.

Steps

Create a FlexCache volume on your Cloud Volumes ONTAP system with an encrypted source volume. For detailed steps and additional considerations, refer to the following sections:

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

Aggregate administration

Create an aggregate for Cloud Volumes ONTAP systems

You can create aggregates yourself or let the NetApp Console 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.

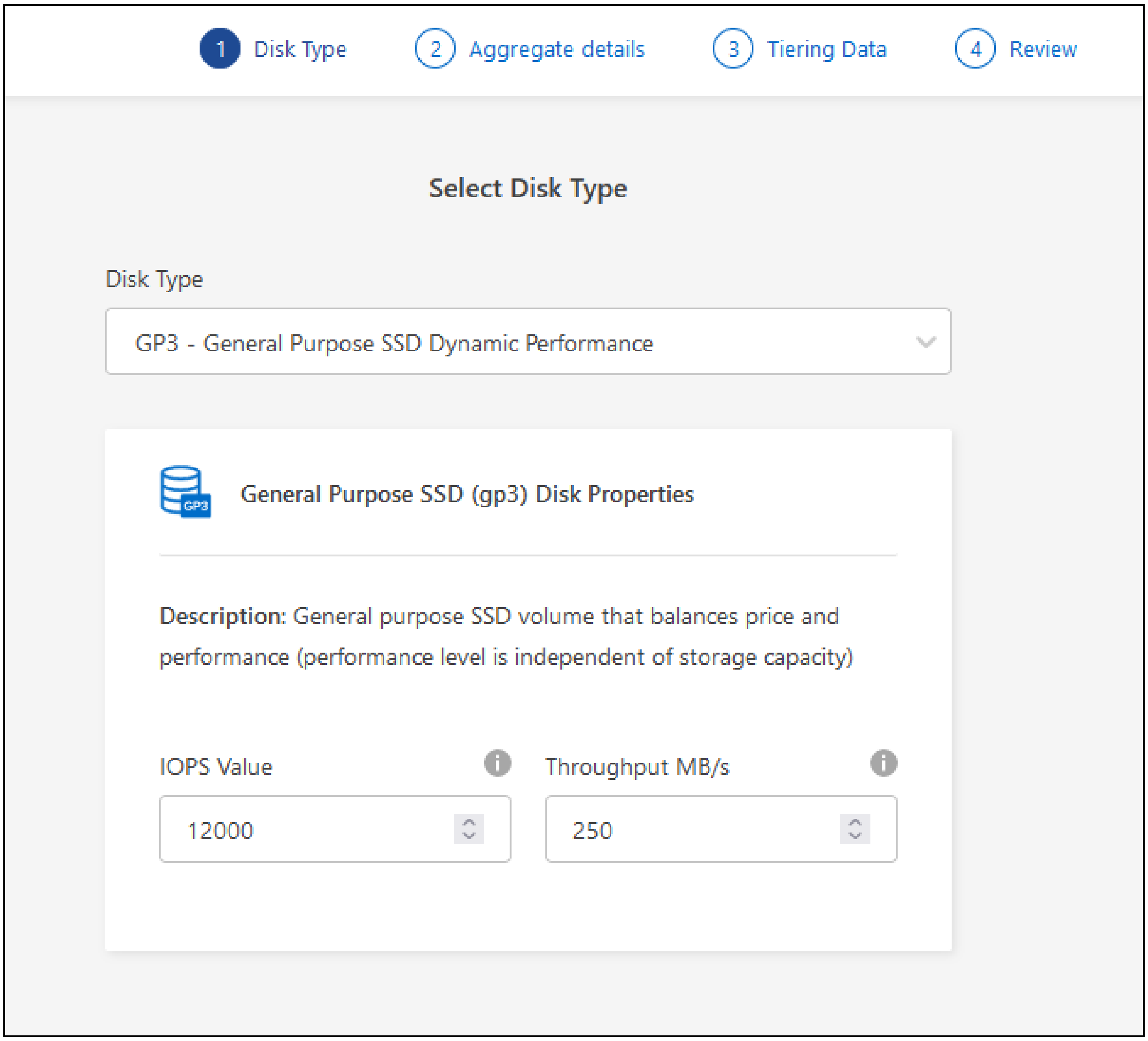
> All disks and aggregates must be created and deleted directly from the Console. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, double-click the name of the Cloud Volumes ONTAP system on which you want to manage aggregates.
3. On the Aggregates tab, click **Add Aggregate** and then specify details for the aggregate.

AWS

- If you're prompted to choose a disk type and disk size, refer to Plan your Cloud Volumes ONTAP configuration in AWS.
- If you're prompted to enter the aggregate's capacity size, then you're creating an aggregate on a configuration that supports the Amazon EBS Elastic Volumes feature. The following screenshot shows an example of a new aggregate comprised of gp3 disks.



Learn more about support for Elastic Volumes.

Azure

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

Google Cloud

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

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

Manage aggregates for Cloud Volumes ONTAP clusters

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 the NetApp Console. 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

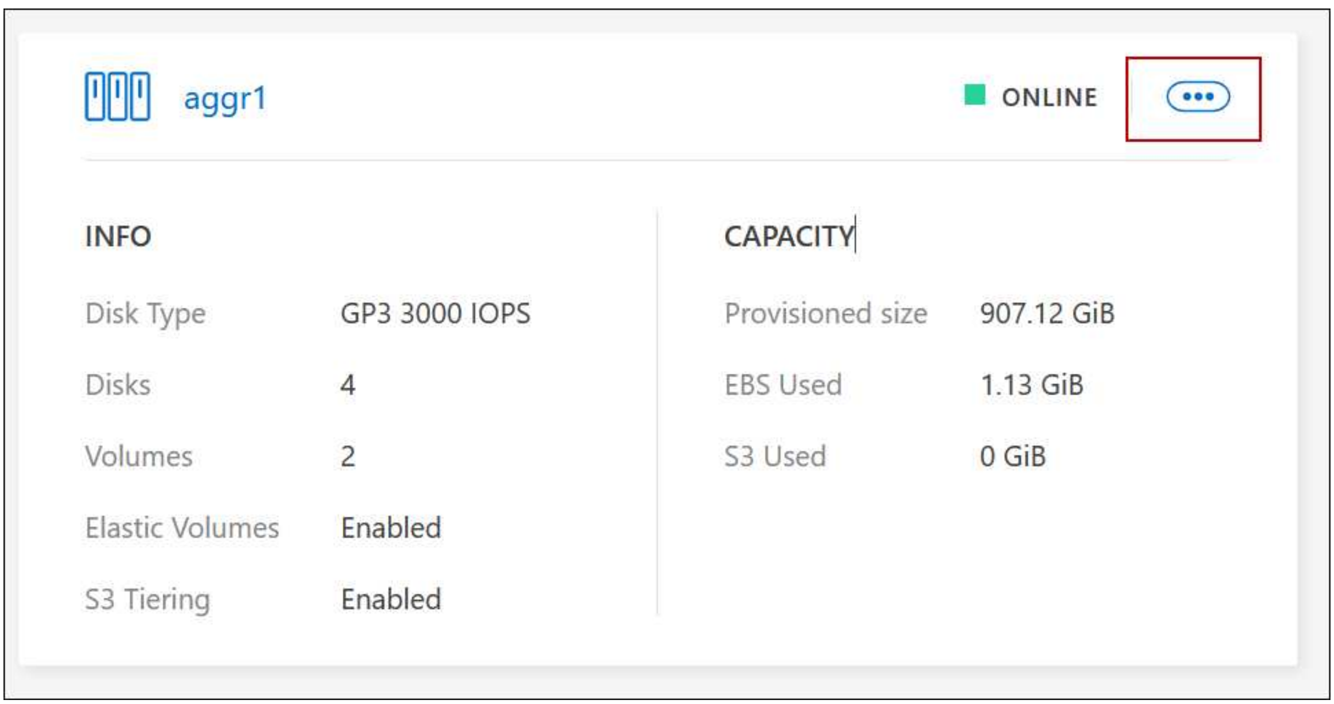
If you want to delete an aggregate, you must have first deleted the volumes in the aggregate.

About this task

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

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, double-click the Cloud Volumes ONTAP system on which you want to manage aggregates.
3. From the system details, click the **Aggregates** tab.
4. For the required aggregate, click the ••• icon for the management actions.



5. Manage your aggregates from the available options in the ••• menu.

> For adding disks to an aggregate, all disks in the aggregate must be of the same size.

For AWS, you can increase the capacity of an aggregate that supports Amazon EBS Elastic Volumes.

a. Under the ••• menu, click **Increase capacity**.

b. Enter the additional capacity that you'd like to add and then click **Increase**.

Note that you must increase the capacity of the aggregate by a minimum of 256 GiB or 10% of the aggregate's size. For example, if you have a 1.77 TiB aggregate, 10% is 181 GiB. That's lower than 256 GiB, so the size of the aggregate must in increased by the 256 GiB minimum.

Manage the Cloud Volumes ONTAP aggregate capacity on a Console agent

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

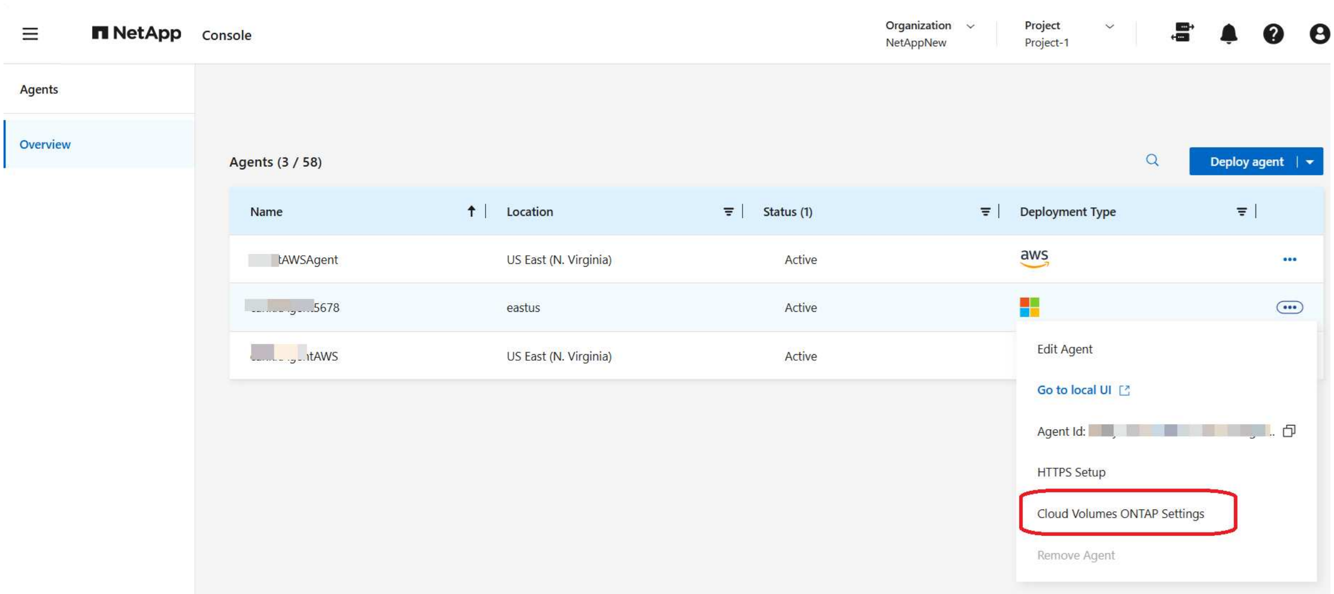
These settings affect all Cloud Volumes ONTAP systems managed by a Console agent. If you have another Console agent, it can be configured differently.

Required permissions

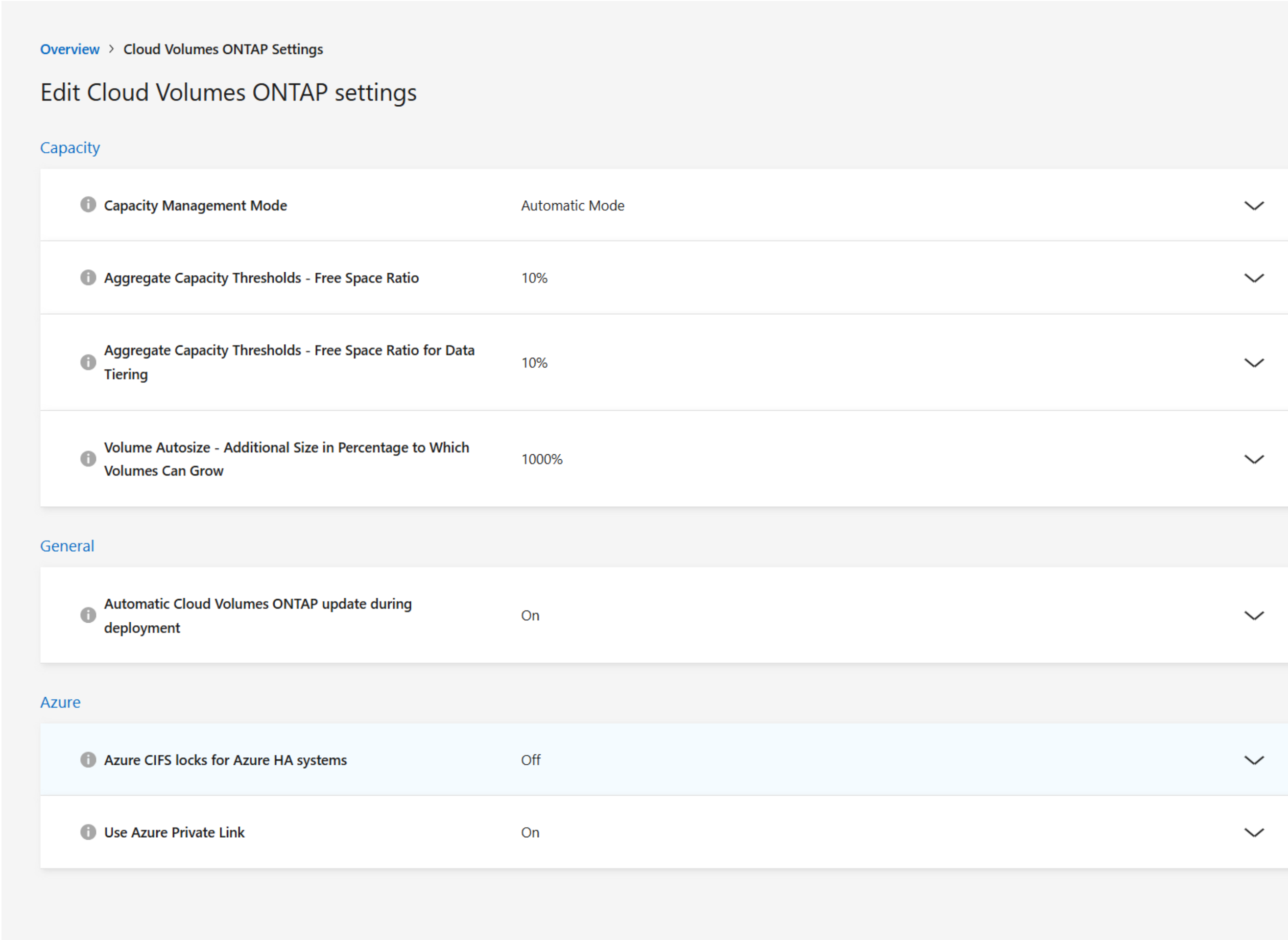
You need the organization or account admin privileges of the NetApp Console to modify Cloud Volumes ONTAP Settings.

Steps

1. From the left navigation pane, go to **Administration > Agents**.
2. Click the ••• icon for the Console agent that manages your Cloud Volumes ONTAP system.
3. Select **Cloud Volumes ONTAP Settings**.



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



Capacity Management Mode

Choose whether the Console should notify you of storage capacity decisions or whether it should automatically manage capacity requirements for you.

Learn how Capacity Management Mode works.

Aggregate Capacity Threshold - Free Space Ratio

This ratio is a key parameter in capacity management decisions, and understanding its impact is essential regardless of whether you are in an automatic or manual mode of capacity management. It is recommended to set this threshold with consideration of your specific storage needs and anticipated growth to maintain a balance between resource utilization and cost.

In the manual mode, if the free space ratio on an aggregate drops below the specified threshold, it triggers a notification, alerting you that you should take actions to address the low free space ratio. It is important to monitor these notifications and manually manage the aggregate capacity to avoid service disruption and ensure optimal performance.

The free space ratio is calculated as follows:
(aggregate capacity - total used capacity on the aggregate) / aggregate capacity

Refer to Automatic capacity management to learn now capacity is automatically managed in Cloud Volumes ONTAP.

Aggregate Capacity Thresholds - 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.

5. Click **Save**.

Manage disk performance in Azure

Manage Premium SSD v2 disk performance for Cloud Volumes ONTAP in Azure

You can optimize Cloud Volumes ONTAP performance in Azure by configuring the IOPS and throughput parameters for Premium SSD v2 disks. This functionality is available only when Cloud Volumes ONTAP is already deployed with Azure Premium SSD v2 disk type, not during the initial deployment. By enhancing performance, you can leverage the full flexibility and high-performance capabilities of Azure Premium SSD v2 disks.

Premium SSD v2 disks support workloads that need fast, reliable performance with low latency, high IOPS, and high throughput. By adjusting the IOPS and throughput settings, you can tailor the performance of the aggregates in your deployment. For more information about Premium SSD v2 disks, refer to Deploy a Premium SSD v2 disk.

Use the APIs to automate the process for modifying Premium SSD v2 disk settings. For information about running Cloud Volumes ONTAP API calls, refer to Your first API call.

About this task

- This feature applies to Cloud Volumes ONTAP deployments in Azure single availability zones.
- Changing the disk settings uniformly modifies the performance of the RAID group or aggregate. The performance of all the disks in the aggregate is adjusted to the same level to ensure consistent performance across the aggregate.
- The changes affect a single aggregate and not other aggregates in a group.
- Premium SSD v2 disks that are provisioned automatically during Cloud Volumes ONTAP deployment or capacity optimization in the NetApp Console, or added through the APIs are all eligible for modification.
- Disk resizing (changing disk capacity) is not supported.

Before you begin

Note these points before configuring the IOPS and throughput parameters for Premium SSD v2 disks:

- Ensure that you have selected Premium SSD v2 data disks only. Premium SSD v1 disks or root and boot disks are not eligible for this change.
- Use the pre-configured baseline settings established by Cloud Volumes ONTAP during deployment as the minimum IOPS and throughput values for the respective disk size. These baseline settings align with the Premium SSD v1 performance characteristics.
- Set IOPS and throughput values at or above the minimum baseline for your disk size. For example, for a 1TB disk size, set the minimum IOPS value to 5,000 and the minimum throughput value to 200 MBps. You can configure values higher than these minimums but not lower.

- Configure values within the supported Premium SSD v2 ranges: IOPS between 3000 and 80000 and throughput between 125 and 1200 MBps.
- Ensure that your Premium SSD v2 disk size is within the supported range of 500GB to 32TB for Cloud Volumes ONTAP in Azure. Note that these size limits differ from the minimum and maximum values offered by Azure for Premium SSD v2 disks.

Steps

- Use the following API call to alter the attribute values for IOPS and throughput:

  > You can invoke this API a maximum of four times within a 24-hour period.

  ```
  PUT /azure/vsa/aggregates/{workingEnvironmentId}/{aggregateName}
  ```

  Include the following parameters in the request body:

  ```
  {
    "aggregateName": "aggr_name",
    "iops": "modified_iops_value",
    "throughput": "modified_throughput_value",
    "workingEnvironmentId": "we_id"
  }
  ```

After you finish

After the API returns a response indicating the operation is successful, verify the modified parameters by checking the disk details in the Azure portal for your Cloud Volumes ONTAP system.

Related information

- Prepare to use the API
- Cloud Volumes ONTAP workflows
- Get required identifiers
- Use REST APIs for Cloud Volumes ONTAP
- Use Premium SSD v2 with VMs in availability set

Change performance tier of Premium SSD disks in Cloud Volumes ONTAP in Azure

You can upgrade the performance tier of Premium SSD managed disks in Cloud Volumes ONTAP in Azure by using the Azure portal. This is a manual process that involves changing the disk tier of each Premium SSD disk to a higher performance tier. Changing the performance tier of your NVRAM disk can help alleviate performance bottlenecks and enhance the efficiency of your Cloud Volumes ONTAP system by providing higher IOPS and throughput capabilities.

> Ensure that you work with NetApp support to determine that the bottleneck that you experience in your environment is due to the NVRAM disk, and upgrading the tier resolves the issue.

About this task

- By default, Cloud Volumes ONTAP in Azure deploys Premium SSD disks for NVRAM in P20 tier. The P20 tier provides a balanced performance suitable for most workloads. However, if your workload demands higher performance, you can upgrade the NVRAM disk to a higher tier such as P30.

> Currently, you can upgrade an NVRAM disk from P20 to P30 tier, only through the Azure portal.

- You do not change the size of the disk. It continues to remain 512 GB. This procedure only changes the disk's performance tier.

Before you begin

- Assess the need for this change carefully, because upgrading the NVRAM disk to a higher performance tier incurs additional costs.
- Your Cloud Volumes ONTAP version must be 9.11.1 or later. For lower versions, you can upgrade to 9.11.1 or later, or raise a Feature Policy Variation Request (FPVR) with NetApp support.

Steps

This scenario assumes that there are two nodes `node01` and `node02` in the Cloud Volumes ONTAP high-availability (HA) deployment. Use the Azure portal to upgrade the tier.

1. Run this command to make `node1` the active node. Manually fail over `node02`.

   ```
   storage failover takeover -ofnode <Node02>
   ```

2. Sign in to the Azure portal.
3. When the takeover is complete, go to the VM instance for `node02`, and click the **Stop** button to switch it off.
4. Navigate to the resource group for `node02` and from the list of disks, select the NVRAM disk to change the tier.
5. Select **Size + Performance**.
6. In the **Performance tier** dropdown, select `P30 - 5000 IOPS, 200MB/s`.
7. Select **Resize**.
8. Switch on the `node02` instance.
9. Check the Azure serial console until you can see the message: `waiting for giveback`.
10. Run this command to give back `node02`:

    ```
    storage failover giveback -ofnode <Node02>
    ```

11. Repeat these steps on `node01` to make `node02` take over `node01`, so that you can upgrade the NVRAM disk tier for `node01`.

After you finish

When you have switched on both the nodes, verify the modified parameters by checking the disk details in the Azure portal for your Cloud Volumes ONTAP system.

Related information

- Azure documentation: Change your performance tier without downtime

- Knowledge base for the support team: How to upgrade performance tier of NVRAM disk in Azure CVO
- Upgrade Cloud Volumes ONTAP software versions

Storage VM administration

Manage storage VMs for Cloud Volumes ONTAP

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.

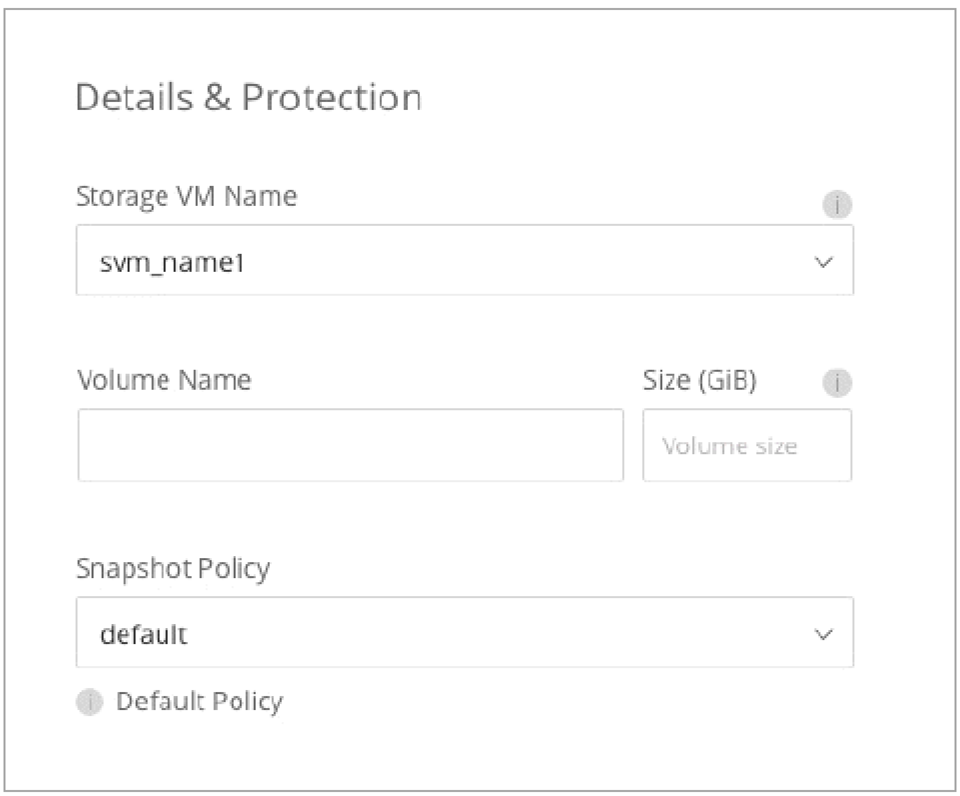
Supported number of storage VMs

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.

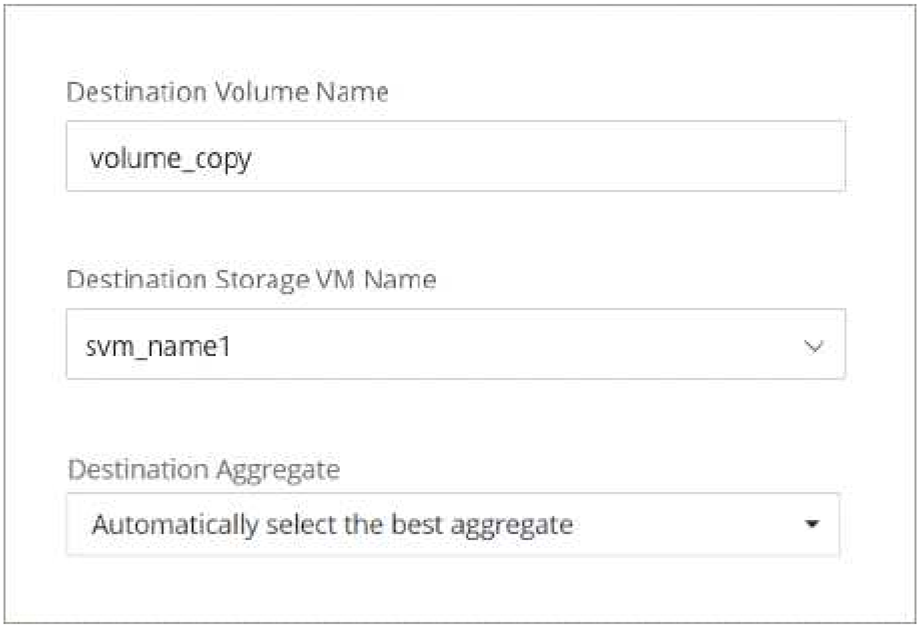
Work with multiple storage VMs

The NetApp Console supports any additional storage VMs that you create from ONTAP System Manager or the ONTAP 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

The Console automatically names the single storage VM that it creates for Cloud Volumes ONTAP. From ONTAP System Manager, the ONTAP CLI, or API, 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.

Manage data-serving storage VMs for Cloud Volumes ONTAP in AWS

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.

To create additional data-serving storage VMs, you need to allocate IP addresses in AWS and then run ONTAP commands based on your Cloud Volumes ONTAP configuration.

Supported number of storage VMs

Multiple storage VMs are supported with specific Cloud Volumes ONTAP configurations starting with the 9.7 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.

Verify limits for your configuration

Each EC2 instance supports a maximum number of private IPv4 addresses per network interface. You need to verify the limit before you allocate IP addresses in AWS for the new storage VM.

Steps

1. Go the Storage limits section in the Cloud Volumes ONTAP Release Notes.

2. Identify the maximum number of IP addresses per interface for your instance type.
3. Make note of this number because you'll need it in the next section when you allocate IP addresses in AWS.

Allocate IP addresses in AWS

Private IPv4 addresses must be assigned to port e0a in AWS before you create LIFs for the new storage VM.

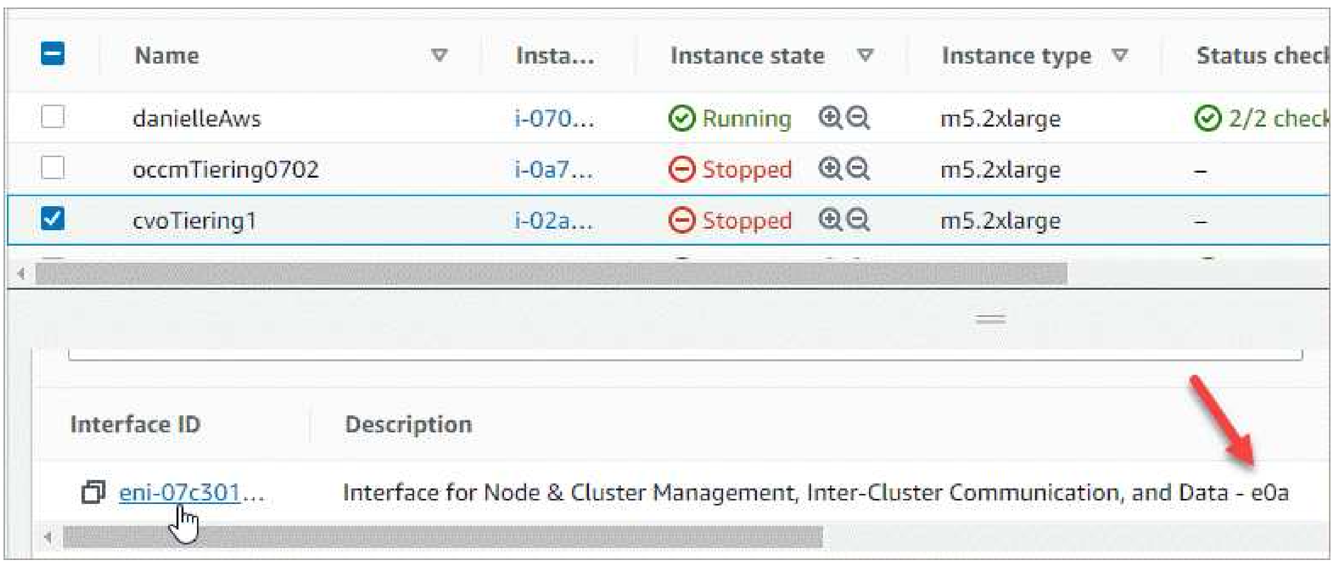
Note that an optional management LIF for a storage VM requires a private IP address on a single-node system and on an HA pair in a single AZ. This management LIF provides a connection to management tools like SnapCenter.

Steps

1. Log in to AWS and open the EC2 service.
2. Select the Cloud Volumes ONTAP instance and click **Networking**.

   If you're creating a storage VM on an HA pair, select node 1.

3. Scroll down to **Network interfaces** and click the **Interface ID** for port e0a.



4. Select the network interface and click **Actions > Manage IP addresses**.
5. Expand the list of IP addresses for e0a.
6. Verify the IP addresses:
   a. Count the number of allocated IP addresses to confirm that the port has room for additional IPs.

      You should have identified the maximum number of supported IP addresses per interface in the previous section of this page.

   b. Optional: Go to the ONTAP CLI for Cloud Volumes ONTAP and run **network interface show** to confirm that each of these IP addresses are in use.

      If an IP address isn't in use, then you can use it with the new storage VM.

7. Back in the AWS Console, click **Assign new IP address** to assign additional IP addresses based on the amount that you need for the new storage VM.

- single-node system: One unused secondary private IP is required.

  An optional secondary private IP is required if you want to create a management LIF on the storage VM.

- HA pair in a single AZ: One unused secondary private IP is required on node 1.

  An optional secondary private IP is required if you want to create a management LIF on the storage VM.

- HA pair in multiple AZs: One unused secondary private IP is required on each node.

8. If you're allocating the IP address on an HA pair in a single AZ, enable **Allow secondary private IPv4 addresses to be reassigned**.
9. Click **Save**.
10. If you have an HA pair in multiple AZs, then you'll need to repeat these steps for node 2.

Create a storage VM on a single-node system

These steps create a new storage VM on a single-node system. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Create a NAS LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node
```

   Where *private_ip_x* is an unused secondary private IP on e0a.

3. Optional: Create a storage VM management LIF.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

   Where *private_ip_y* is another unused secondary private IP on e0a.

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.

Create a storage VM on an HA pair in a single AZ

These steps create a new storage VM on an HA pair in a single AZ. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

Both of these LIFs get allocated on node 1. The private IP addresses can move between nodes if failures occur.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

Where *private_ip_x* is an unused secondary private IP on e0a of cvo-node1. This IP address can be relocated to the e0a of cvo-node2 in case of takeover because the service policy default-data-files indicates that IPs can migrate to the partner node.

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

Where *private_ip_y* is another unused secondary private IP on e0a.

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
```

Create a storage VM on an HA pair in multiple AZs

These steps create a new storage VM on an HA pair in multiple AZs.

A *floating* IP address is required for a NAS LIF and is optional for a management LIF. These floating IP addresses don't require you to allocate private IPs in AWS. Instead, the floating IPs are automatically configured in the AWS route table to point to a specific node's ENI in the same VPC.

In order for floating IPs to work with ONTAP, a private IP address must be configured on every storage VM on each node. This is reflected in the steps below where an iSCSI LIF is created on node 1 and on node 2.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

   - The floating IP address must be outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. 192.168.209.27 is an example floating IP address. Learn more about choosing a floating IP address.
   - `-service-policy default-data-files` indicates that IPs can migrate to the partner node.

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. Create an iSCSI LIF on node 1.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

   - This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
   - `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.

    - *private_ip* is an unused secondary private IP address on eth0 (e0a) of cvo_node1.
5. Create an iSCSI LIF on node 2.

   ```
   network interface create -vserver svm_2 -service-policy default-data-
   blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
   ip_node2_iscsi_2 -home-node cvo-node2
   ```

    - This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
    - `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.
    - *private_ip* is an unused secondary private IP address on eth0 (e0a) of cvo_node2.
6. 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.

7. 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
```

Manage 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 you can create additional storage VMs when running Cloud Volumes ONTAP in Azure.

To create and manage additional data-serving storage VMs in Azure, you should use the APIs. This is because the APIs automate the process of creating the storage VMs and configuring the required network interfaces. When creating the storage VMs, the NetApp Console configures the required LIF services, as well as an iSCSI LIF that's required for outbound SMB/CIFS communications from the storage VM.

For information about running Cloud Volumes ONTAP API calls, refer to Your first API call.

Supported number of storage VMs

Beginning with Cloud Volumes ONTAP 9.9.0, based on your license, multiple storage VMs are supported with specific configurations. Refer to the Cloud Volumes ONTAP Release Notes to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All versions of Cloud Volumes ONTAP prior to 9.9.0 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.

Create a storage VM

Based on your configuration and license type, you can create multiple storage VMs on a single-node system or in a high-availability (HA) configuration by using the APIs for the NetApp Console.

About this task

When you create storage VMs using the APIs, along with configuring the required network interfaces, the Console also modifies the `default-data-files` policies on the data storage VMs by removing the following services from the NAS data LIF and adding them to the iSCSI data LIF that's used for outbound management connections:

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

Before you begin

The Console agent requires specific permissions to create storage VMs for Cloud Volumes ONTAP. The required permissions are included in the policies provided by NetApp.

single-node system

Use the following API call to create a storage VM on a single-node system.

`POST /azure/vsa/working-environments/{workingEnvironmentId}/svm`

Include the following parameters in the request body:

```
{ "svmName": "myNewSvm1"
   "svmPassword": "optional, the API takes the cluster password if not
provided"
   "mgmtLif": "optional, to create an additional management LIF, if you
want to use the storage VM for management purposes"}
```

HA pair

Use the following API call to create a storage VM on an HA pair:

```
POST /azure/ha/working-environments/{workingEnvironmentId}/svm
```

Include the following parameters in the request body:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

Manage storage VMs on single-node systems and HA pairs

Using the APIs, you can rename and delete storage VMs in both single node and HA configurations.

Before you begin

The Console agent requires specific permissions to manage storage VMs for Cloud Volumes ONTAP. The required permissions are included in the policies provided by NetApp.

Rename a storage VM

To rename a storage VM, you should provide the names of the existing storage VM and new storage VM as parameters.

Steps

- Use the following API call to rename a storage VM on a single-node system:

  ```
  PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm
  ```

  Include the following parameters in the request body:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- Use the following API call to rename a storage VM on an HA pair:

  ```
  PUT /azure/ha/working-environments/{workingEnvironmentId}/svm
  ```

  Include the following parameters in the request body:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

Delete a storage VM

In a single node or HA configuration, you can remove a storage VM if it doesn't have any active volumes.

Steps

- Use the following API call to delete a storage VM on a single-node system:

```
DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- Use the following API call to delete a storage VM on an HA pair:

```
DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

Related information

- Prepare to use the API
- Cloud Volumes ONTAP workflows
- Get required identifiers
- Use the REST APIs for NetApp Console

Manage data-serving storage VMs for Cloud Volumes ONTAP in Google Cloud

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.

To create and manage additional data-serving storage VMs in Google Cloud, you should use the APIs. This is because the APIs automate the process of creating the storage VMs and configuring the required network interfaces. When creating the storage VMs, the NetApp Console configures the required LIF services, as well as an iSCSI LIF that's required for outbound SMB/CIFS communications from the storage VM.

For information about running Cloud Volumes ONTAP API calls, refer to Your first API call.

Supported number of storage VMs

Beginning with Cloud Volumes ONTAP 9.11.1, based on your license, multiple storage VMs are supported with specific configurations. Refer to the Cloud Volumes ONTAP Release Notes to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All versions of Cloud Volumes ONTAP prior to 9.11.1 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.

Create a storage VM

Based on your configuration and license type, you can create multiple storage VMs on a single-node system or in a high-availability (HA) configuration by using the APIs.

About this task

When you create storage VMs using the APIs, along with configuring the required network interfaces, the Console also modifies the `default-data-files` policies on the data storage VMs by removing the following services from the NAS data LIF and adding them to the iSCSI data LIF that's used for outbound management connections:

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

Before you begin

The Console agent requires specific permissions to create storage VMs for Cloud Volumes ONTAP HA pairs. The required permissions are included in the policies provided by NetApp.

single-node system

Use the following API call to create a storage VM on a single-node system.

```
POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

Include the following parameters in the request body:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

HA pair

Use the following API call to create a storage VM on an HA pair:

```
POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/
```

Include the following parameters in the request body:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

Manage storage VMs

Using the APIs, you can rename and delete storage VMs in both single node and HA configurations.

Before you begin

The Console agent requires specific permissions to manage storage VMs for Cloud Volumes ONTAP HA pairs. The required permissions are included in the policies provided by NetApp.

Rename a storage VM

To rename a storage VM, you should provide the names of the existing storage VM and new storage VM as parameters.

Steps

- Use the following API call to rename a storage VM on a single-node system:

  `PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm`

  Include the following parameters in the request body:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- Use the following API call to rename a storage VM on an HA pair:

  `PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm`

  Include the following parameters in the request body:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

Delete a storage VM

In a single node or HA configuration, you can remove a storage VM if it doesn’t have any active volumes.

Steps

- Use the following API call to delete a storage VM on a single-node system:

  `DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}`

- Use the following API call to delete a storage VM on an HA pair:

  `DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}`

Related information

- Prepare to use the API
- Cloud Volumes ONTAP workflows
- Get required identifiers
- Use the REST APIs for the NetApp Console

Set up storage VM disaster recovery for Cloud Volumes ONTAP

The NetApp Console does not offer setup or orchestration support for storage VM (SVM) disaster recovery. To perform these tasks, use ONTAP System Manager or the ONTAP CLI.

If you set up SnapMirror SVM replication between two Cloud Volumes ONTAP systems, the replication must be between two HA pair systems or two single-node systems. You can't set up SnapMirror SVM replication between an HA pair and a single-node system.

Refer to the following documents for the ONTAP CLI instructions.

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

Security and data encryption

Encrypt volumes on Cloud Volumes ONTAP 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:

- AWS Key Management Service (beginning in 9.12.0)
- Azure Key Vault (AKV)
- Google Cloud Key Management Service

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.

Before you begin

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 the Console
- Register pay-as-you-go systems

> The NetApp Console 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.
   - AWS: AWS Key Management Service
   - Azure: Azure Key Vault (AKV)
   - Google Cloud: Google Cloud Key Management Service

Manage Cloud Volumes ONTAP encryption keys with AWS Key Management Service

You can use AWS's Key Management Service (KMS) to protect your ONTAP encryption keys in an AWS-deployed application.

Key management with the AWS KMS can be enabled with the CLI or the ONTAP REST API.

When using the KMS, be aware that by default a data SVM's LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with AWS's authentication services. If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

Before you begin

- Cloud Volumes ONTAP must be running version 9.12.0 or later
- You must have installed the Volume Encryption (VE) license and
- You must have installed the Multi-tenant Encryption Key Management (MTEKM) license installed.
- You must be a cluster or SVM administrator
- You must have an active AWS subscription

You can only configure keys for a data SVM.

Configuration

AWS

1. You must create a grant for the AWS KMS key that will be used by the IAM role managing encryption. The IAM role must include a policy that allows the following operations:
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`

   To create a grant, refer to AWS documentation.
2. Add a policy to the appropriate IAM role. The policy should support the `DescribeKey`, `Encrypt`, and `Decrypt` operations.

Cloud Volumes ONTAP

1. Switch to your Cloud Volumes ONTAP environment.

2. Switch to the advanced privilege level:
   `set -privilege advanced`
3. Enable the AWS key manager:
   `security key-manager external aws enable -vserver *data_svm_name* -region *AWS_region* -key-id *key_ID* -encryption-context *encryption_context*`
4. When prompted, enter the secret key.
5. Confirm the AWS KMS was configured correctly:
   `security key-manager external aws show -vserver *svm_name*`

Manage Cloud Volumes ONTAP encryption keys with Azure Key Vault

You can use Azure Key Vault (AKV) to protect your ONTAP encryption keys in an Azure-deployed application. Refer to the Microsoft documentation.

AKV can be used to protect NetApp Volume Encryption (NVE) keys only for data SVMs. For more information, refer to the ONTAP documentation.

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.

Before you begin

- 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)
- You must have a Multi-tenant Encryption Key Management (MT_EK_MGMT) license
- You must be a cluster or SVM administrator
- An Active Azure subscription

Limitations

- AKV can only be configured on a data SVM
- NAE can't be used using AKV. NAE requires an external-supported KMIP server.
- Cloud Volumes ONTAP nodes poll AKV every 15 minutes to confirm accessibility and key availability. This polling period is non-configurable, and after four consecutive failures in the polling attempt (totaling 1 hour), the volumes are placed offline.

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 Azure Key Vault app registration, select the **Certificates & 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. Click **Add** to create the client secret. Copy the secret string listed in the **Value** column and store it in a secure location for use later in Cloud Volumes ONTAP configuration. The secret value will not be displayed again after you navigate away from the page.

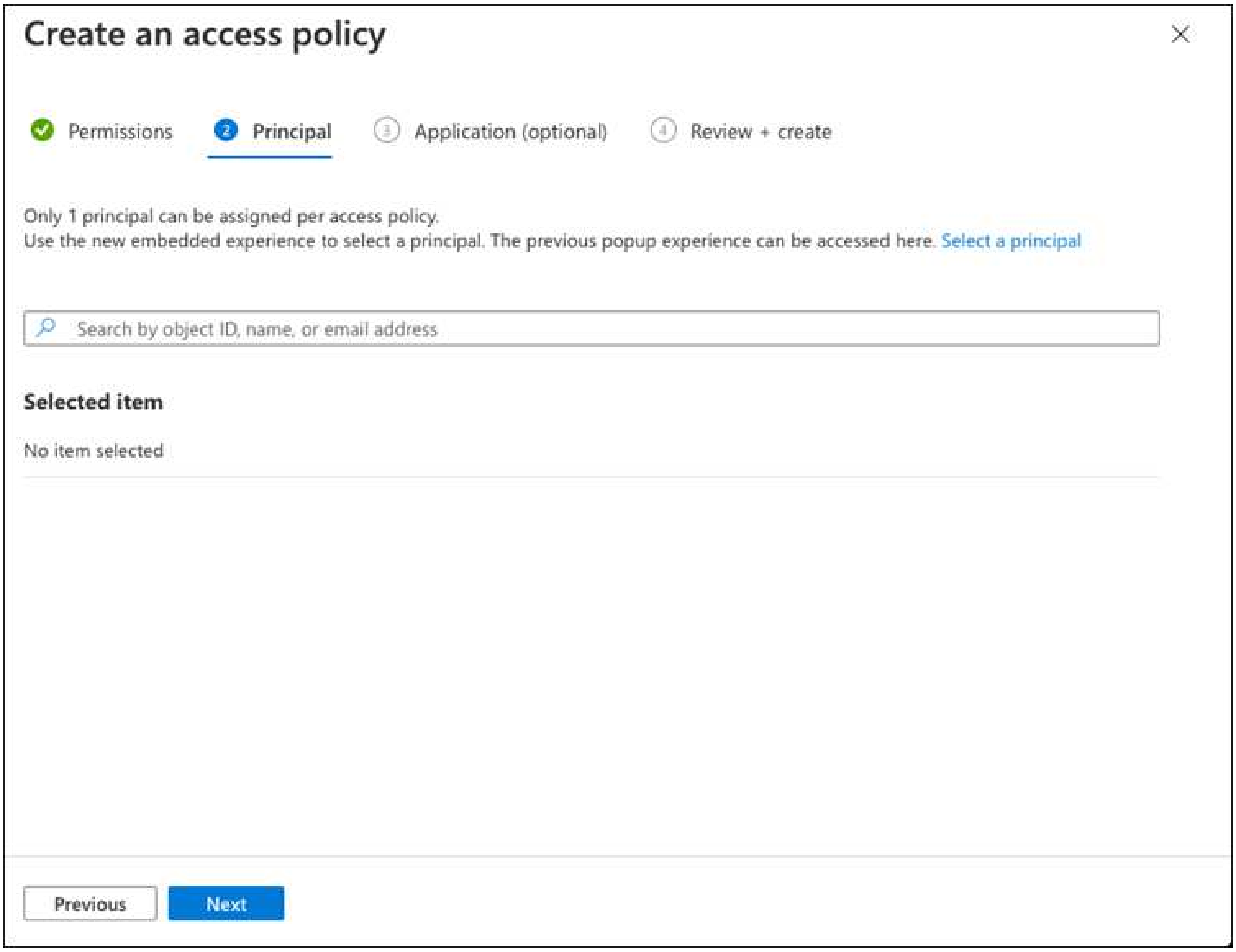
Create an Azure Key Vault

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. Click **+Create** and enter the required information including resource group, region, and pricing tier. In addition, enter the number of days to retain deleted vaults and select **Enable purge protection** on the key vault.
4. Select **Next** to choose an access policy.
5. Select the following options:
    a. Under **Access configuration**, select the **Vault access policy**.
    b. Under **Resource access**, select **Azure Disk Encryption for volume encryption**.
6. Select **+Create** to add an access policy.
7. Under **Configure from a template**, click the drop-down menu and then select the **Key, Secret, and Certificate Management** template.
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**: 20 selected
    - **Secret permissions**: 8 selected
    - **Certificate permissions**: 16 selected


Create an access policy
Permissions
Principal
Application (optional)
Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. Click **Next** to select the **Principal** Azure registered application you created in Azure Application Registration. Select **Next**.

   Only one principal can be assigned per policy.



10. Click **Next** two times until you arrive at **Review and create**. Then, click **Create**.
11. Select **Next** to advance to **Networking** options.
12. 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.)
13. 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 need this for a later step.

Create encryption key

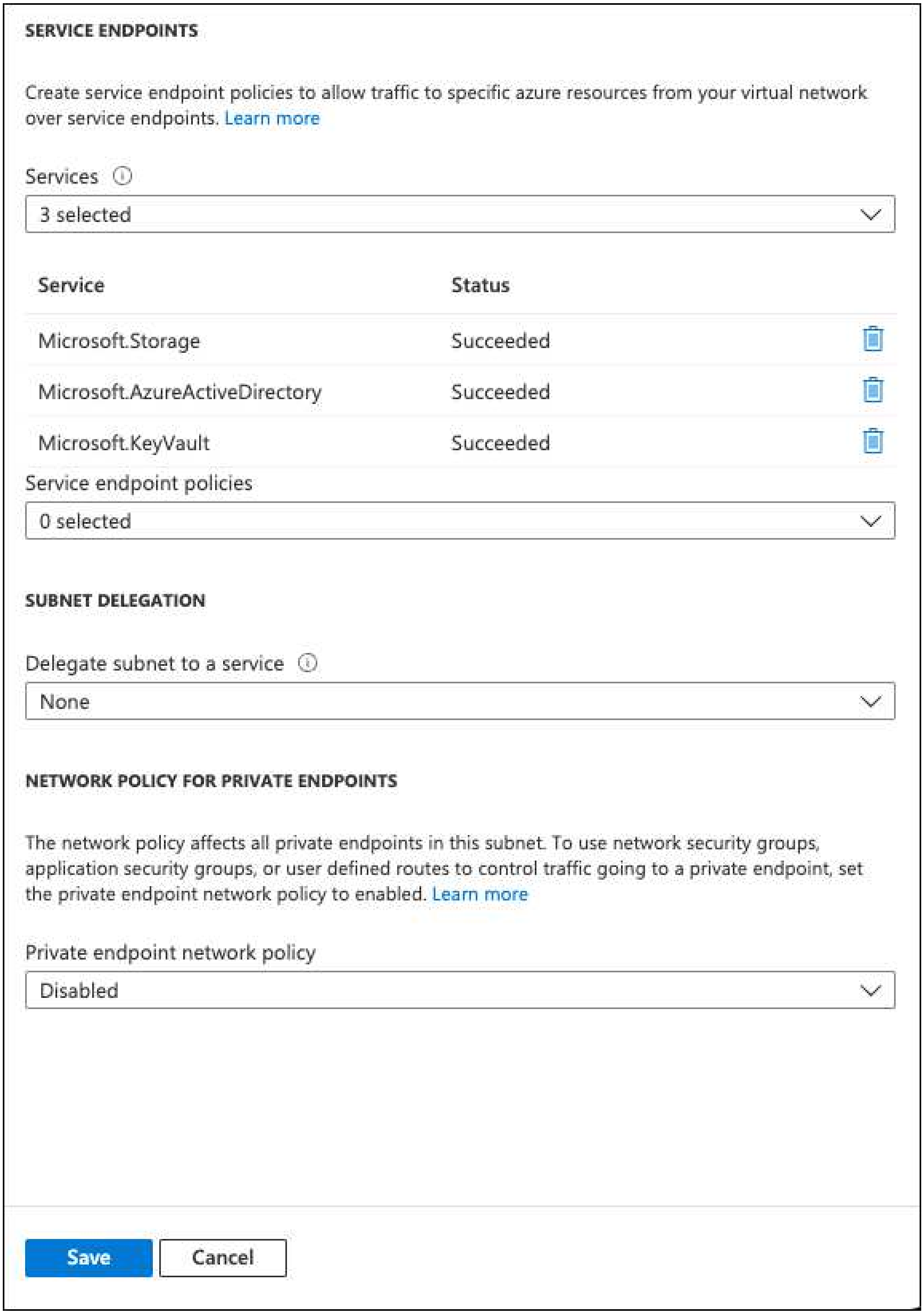
1. In the menu for the Key Vault you have created for Cloud Volumes ONTAP, navigate to the **Keys** option.
2. Select **Generate/import** to create a new key.
3. Leave the default option set to **Generate**.
4. Provide the following information:
   - Encryption key name

- 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 system.
2. In the Azure portal navigate to **Virtual Networks**.
3. Select the Virtual Network where you deployed the Cloud Volumes ONTAP system 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 drop-down menu, select the following:
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage** (optional)



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 key_vault_URI -key-id full_key_URI`

   > The `_full_key_URI` value must utilize the `<https:// <key vault host name>/keys/<key label>` format.

5. Upon successful enablement of the Azure Key Vault, enter the `client secret value` when prompted.
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. Ensure that your Azure network policies and routing don't block your private vNet from reaching the Azure Key Vault Public endpoint. If they do, consider using an Azure Private endpoint to access the Key vault from within the vNet. You may also need to add a static hosts entry on your SVM to resolve the private IP address for your endpoint.

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`

9. Optional: If you want to update the credentials on the Azure Key Vault authentication certificate, use the following command:
   ```
   security key-manager external azure update-credentials -vserver v1
   -authentication-method certificate
   ```

Related links

- Set up Cloud Volumes ONTAP to use a customer-managed key in Azure
- Microsoft Azure docmentation: About Azure Key Vault
- ONTAP command reference guide

Manage Cloud Volumes ONTAP encryption keys with Google Cloud KMS

You can use Google Cloud Platform's Key Management Service (Cloud KMS) to protect your Cloud Volumes ONTAP encryption keys in a Google Cloud Platform-deployed application.

Key management with Cloud KMS can be enabled with the ONTAP CLI or the ONTAP REST API.

When using Cloud KMS, be aware that by default a data SVM's 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 (oauth2.googleapis.com). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

Before you begin

- Your system should be running Cloud Volumes ONTAP 9.10.1 or later
- You must use a data SVM. Cloud KMS can be configured only on a data SVM.
- You must be a cluster or SVM administrator
- Volume Encryption (VE) license should be installed on the SVM
- Beginning with Cloud Volumes ONTAP 9.12.1 GA, the multi-tenant Encryption Key Management (MTEKM) license should also be installed
- An active Google Cloud Platform subscription is required

Configuration

Google Cloud

1. In your Google Cloud environment, create a symmetric GCP key ring and key.
2. Assign a custom role to the Cloud KMS key and Cloud Volumes ONTAP service account.
   a. Create the custom role:

      ```
      gcloud iam roles create kmsCustomRole
          --project=<project_id>
          --title=<kms_custom_role_name>
          --description=<custom_role_description>

      --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersio
      ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
      sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
      dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
      et
          --stage=GA
      ```

   b. Assign the custom role you created:

      ```
      gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
      --location key_location --member serviceAccount:_service_account_Name_
      --role projects/customer_project_id/roles/kmsCustomRole
      ```

      If you are on Cloud Volumes ONTAP 9.13.0 or later, you don't need to create a custom role. You can assign the predefined `cloudkms.cryptoKeyEncrypterDecrypter` role.

3. Download service account JSON key:

   ```
   gcloud iam service-accounts keys create key-file --iam-account=sa-name
   @project-id.iam.gserviceaccount.com
   ```

Cloud Volumes ONTAP

1. Connect to the cluster management LIF with your preferred SSH client.
2. Switch to the advanced privilege level:

   ```
   set -privilege advanced
   ```

3. Create a DNS for the data SVM.

   ```
   dns create -domains c.<project>.internal -name-servers server_address -vserver
   SVM_name
   ```

4. Create CMEK entry:

   ```
   security key-manager external gcp enable -vserver SVM_name -project-id project
   -key-ring-name key_ring_name -key-ring-location key_ring_location -key-name
   key_name
   ```

5. When prompted, enter the service account JSON key from your GCP account.
6. Confirm the enabled process succeeded:

   ```
   security key-manager external gcp check -vserver svm_name
   ```

7. OPTIONAL: Create a volume to test encryption `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

Troubleshoot

If you need to troubleshoot, you can tail the raw REST API logs in the final two steps above:

1. `set d`
2. `systemshell -node *node* -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Enable NetApp ransomware protection solutions for Cloud Volumes ONTAP

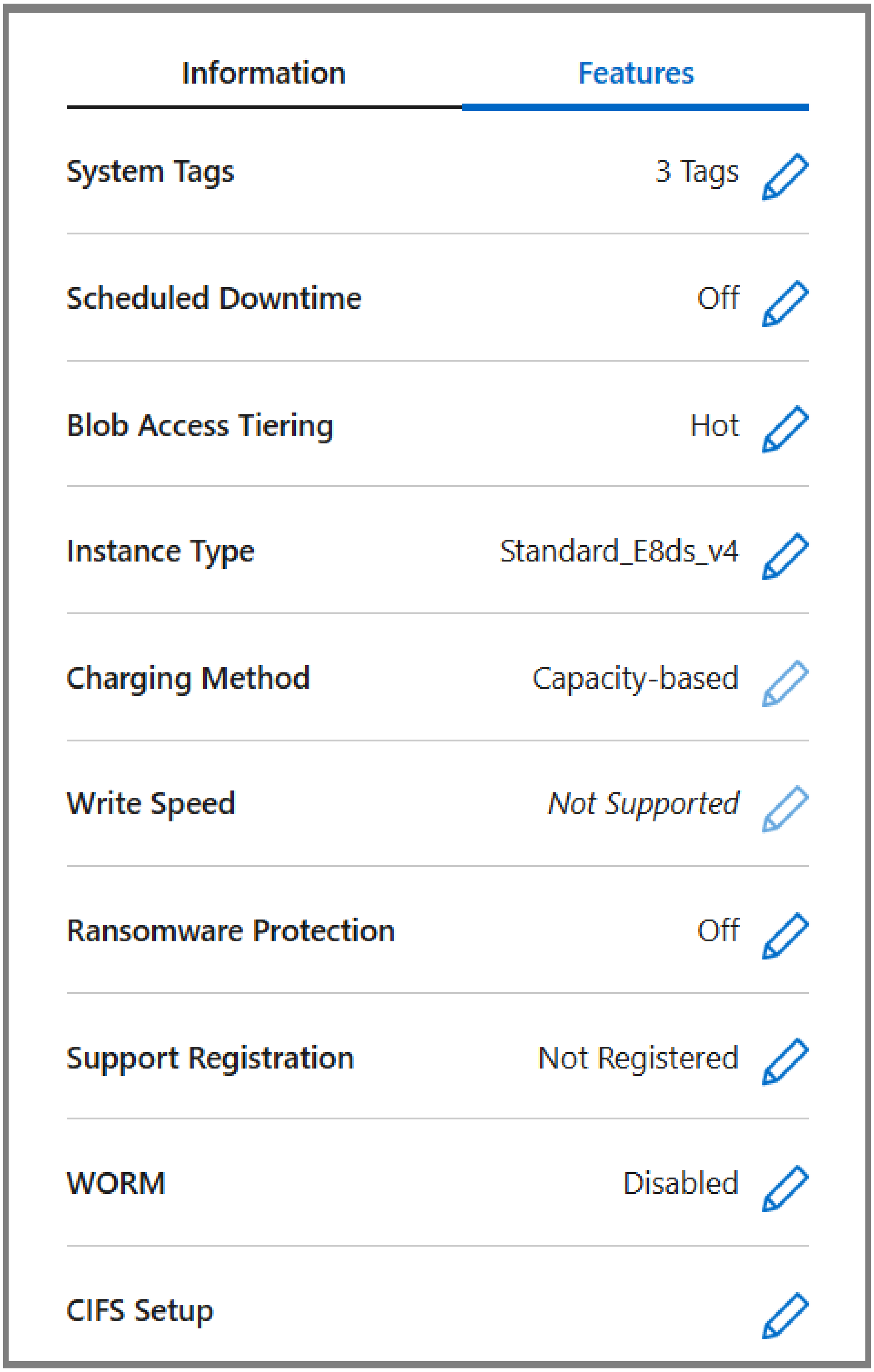
Ransomware attacks can cost a business time, resources, and reputation. The NetApp Console enables you to implement two NetApp solutions for ransomware: Protection from common ransomware file extensions and Autonomous Ransomware Protection (ARP). These solutions provide effective tools for visibility, detection, and remediation.

Protection from common ransomware file extensions

Available on the Console, the Ransomware Protection setting allows you to utilize the ONTAP FPolicy functionality to guard against common ransomware file extension types.

Steps

1. On the **Systems** page, double-click the name of the Cloud Volumes ONTAP system you configure to use ransomware protection.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Ransomware Protection**.



3. 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.

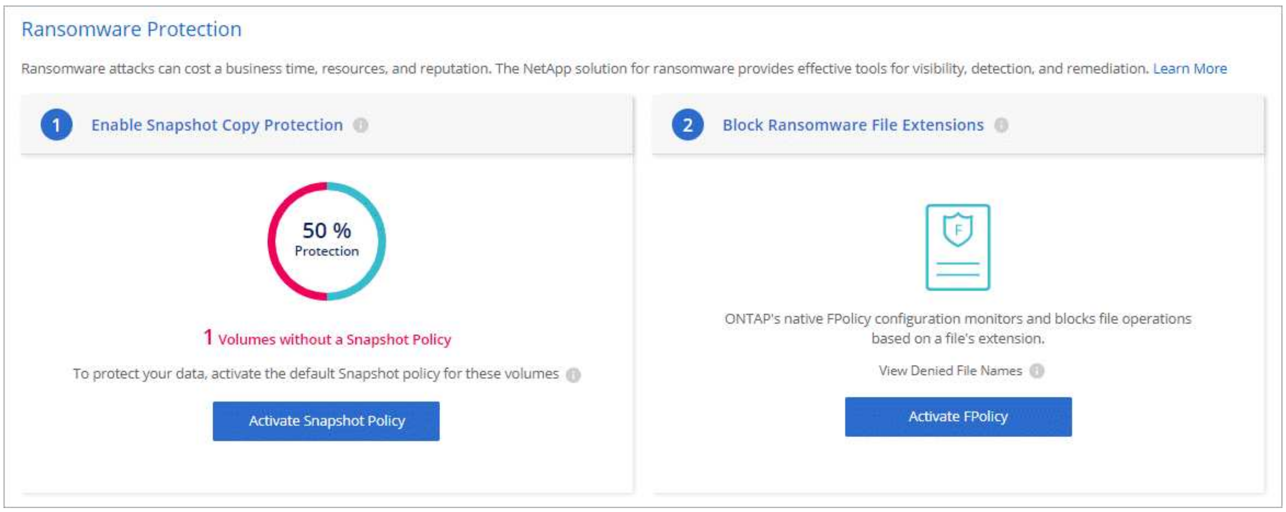
    b. Click **Activate FPolicy** to enable ONTAP's FPolicy solution, which can block file operations based on a file’s extension.

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

> This scope is created 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.



Autonomous Ransomware Protection

Cloud Volumes ONTAP supports the Autonomous Ransomware Protection (ARP) feature, which performs analyses on workloads to proactively detect and warn about abnormal activity that might indicate a ransomware attack.

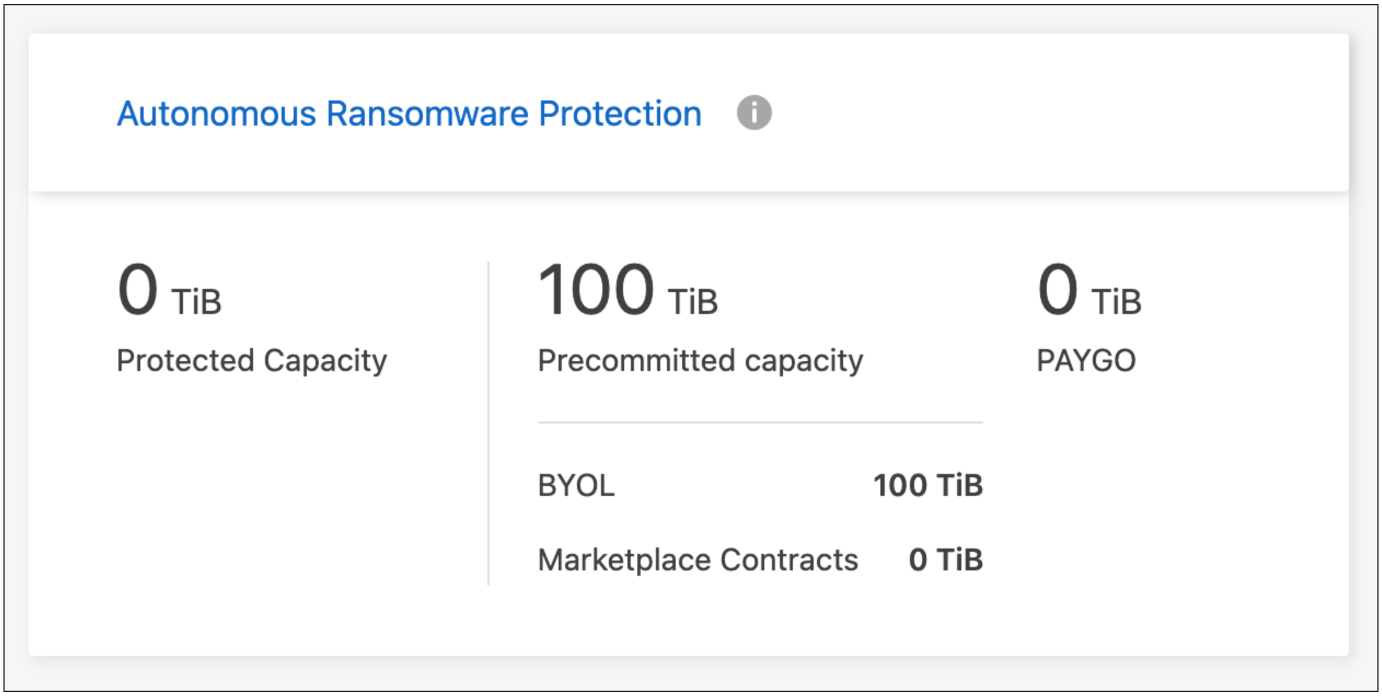
Separate from the file extension protections provided through the ransomware protection setting, the ARP feature uses workload analysis to alert the user on potential attacks based on detected “abnormal activity”. Both the ransomware protection setting and the ARP feature can be used in conjunction for comprehensive ransomware protection.

The ARP feature is available for use with bring your own license (BYOL) and marketplace subscriptions for your licenses at no additional cost.

ARP-enabled volumes have a designated state of "Learning mode" or "Active".

Configuration of ARP for volumes is performed through ONTAP System Manager and ONTAP CLI.

For more information on how to enable ARP with ONTAP System Manager and the ONTAP CLI, refer to the ONTAP documentation: Enable Autonomous Ransomware Protection.



Create tamperproof Snapshot copies of WORM files on Cloud Volumes ONTAP

You can create tamperproof Snapshot copies of write once, read many (WORM) files on a Cloud Volumes ONTAP system and retain the snapshots in unmodified form for a specific retention period. This functionality is powered by the SnapLock technology, and provides an additional layer of data protection and compliance.

Before you begin

Ensure that the volume that you use for creating Snapshot copies is a SnapLock volume. For information about enabling SnapLock protection on volumes, refer to the ONTAP documentation: Configure SnapLock.

Steps

1. Create Snapshot copies from the SnapLock volume. For information about creating Snapshot copies by using the CLI or System Manager, refer to the ONTAP documentation: Manage local Snapshot copies overview.

   The Snapshot copies inherit the WORM properties of the volume, making them tamperproof. The underlying SnapLock technology ensures that a snapshot remains protected from edit and deletion until the specified retention period has elapsed.

2. You can modify the retention period if there's a need to edit these snapshots. For information, refer to the ONTAP documentation: Set the retention time.

> Even though a Snapshot copy is protected for a specific retention period, the source volume can be deleted by a cluster administrator, as WORM storage in Cloud Volumes ONTAP operates under a "trusted storage administrator" model. Additionally, a trusted cloud administrator can delete the WORM data by operating on the cloud storage resources.

Related links

- For more information about WORM, refer to Learn about WORM storage on Cloud Volumes ONTAP.

* For information about charging of SnapLock volumes, refer to Licensing and charging in Cloud Volumes ONTAP.

System administration

Upgrade Cloud Volumes ONTAP

Upgrade Cloud Volumes ONTAP from the NetApp Console 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 Console only

You should not upgrade Cloud Volumes ONTAP by using ONTAP System Manager or the ONTAP CLI, but only the Console. Otherwise, it might impact system stability.

The Console provides two ways to upgrade Cloud Volumes ONTAP:

* By following upgrade notifications that appear on the system
* By placing the upgrade image at an HTTPS location and then providing the Console with the URL

Supported upgrade paths

The Cloud Volumes ONTAP version you can upgrade to depends on the version you are currently running. Each generic or patch version in a release in the following tables represents the base version available for upgrade. For details about the available patches, refer to the versioned release notes for each release.

Supported upgrade paths for AWS

Current version	Versions that you can directly upgrade to
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1

Current version	Versions that you can directly upgrade to
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
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

Supported upgrade paths for Azure

Current version	Versions that you can directly upgrade to
9.17.1 P1	9.18.1
9.16.1 P3	9.17.1 P1
9.15.1 P10	9.16.1 P3
9.14.1 P13	9.15.1 P10
9.13.1 P16	9.14.1 P13
9.12.1 P18	9.13.1 P16
9.11.1 P20	9.12.1 P18

If you have a lower version of Cloud Volumes ONTAP in Azure, you must first upgrade to the next version and follow the supported upgrade paths to reach your target version. For example, if you have Cloud Volumes ONTAP 9.7 P7, follow this upgrade path:

- 9.7 P7 → 9.8 P18
- 9.8 P18 → 9.9.1 P15
- 9.9.1 P15 → 9.10.1 P12
- 9.10.1 P12 → 9.11.1 P20

Supported upgrade paths for Google Cloud

Current version	Versions that you can directly upgrade to
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
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

Current version	Versions that you can directly upgrade to
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 notifications that appear in a system, the Console 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.

Patch releases

Starting in January 2024, patch upgrades are only available if there's a patch release for the three latest versions of Cloud Volumes ONTAP. Patch versions are occasionally available for deployment, when the RC or GA version isn't available for deployment.

We use the latest GA release to determine the three latest versions to display in the Console. For example, if the current GA release is 9.13.1, patches for 9.11.1-9.13.1 appear in the Console.

For patch versions 9.11.1 or below, you will need to use a manual upgrade procedure by downloading the ONTAP image.

As a general rule for patch releases, you can upgrade from a lower patch version to any higher patch version in the same or the next Cloud Volumes ONTAP release.

Here are a couple of examples:

- 9.13.0 → 9.13.1 P15
- 9.12.1 → 9.13.1 P2

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 pay-as-you-go (PAYGO) and bring your own license (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 the Console 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

The Console also updates the mediator instance as needed during the Cloud Volumes ONTAP upgrade process.

Upgrades in AWS with c4, m4, and r4 EC2 instance types

Cloud Volumes ONTAP no longer supports the c4, m4, and r4 EC2 instance types. You can upgrade existing deployments to Cloud Volumes ONTAP versions 9.8-9.12.1 with these instance types. Before you upgrade we recommend that you change the instance type. If you can't change the instance type, you need to enable enhanced networking before you upgrade. Read the following sections to learn more about changing the instance type and enabling enhanced networking.

In Cloud Volumes ONTAP running versions 9.13.0 and above, you cannot upgrade with c4, m4, and r4 EC2 instance types. In this case, you need to reduce the number of disks and then change the instance type or deploy a new HA-pair configuration with the c5, m5, and r5 EC2 instance types and migrate the data.

Change the instance type

c4, m4, and r4 EC2 instance types allow for more disks per node than the c5, m5, and r5 EC2 instance types. If the disk count per node for the c4, m4, or r4 EC2 instance you're running is below the max disk allowance per node for c5, m5, and r5 instances, you can change the EC2 instance type to c5, m5, or r5.

Check disk and tiering limits by EC2 instance
Change the EC2 instance type for Cloud Volumes ONTAP

If you can't change the instance type, follow the steps in Enable enhanced networking.

Enable enhanced networking

To upgrade to Cloud Volumes ONTAP versions 9.8 and later, you must enable *enhanced networking* on the cluster running the c4, m4, or r4 instance type. To enable ENA, refer to the Knowledge Base article "How to enable Enhanced networking like SR-IOV or ENA on AWS Cloud Volumes ONTAP instances".

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

* Verify that all LIFs are on home ports

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.

In many cases, 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.

Session-oriented protocols might cause adverse effects on clients and applications in certain areas during upgrades. For details, refer to the ONTAP documentation

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 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 NetApp Backup and Recovery 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 ONTAP 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 system.

   > The computer from which you are accessing the Console must have a network connection to Cloud Volumes ONTAP. For example, you might need to log in to the Console 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

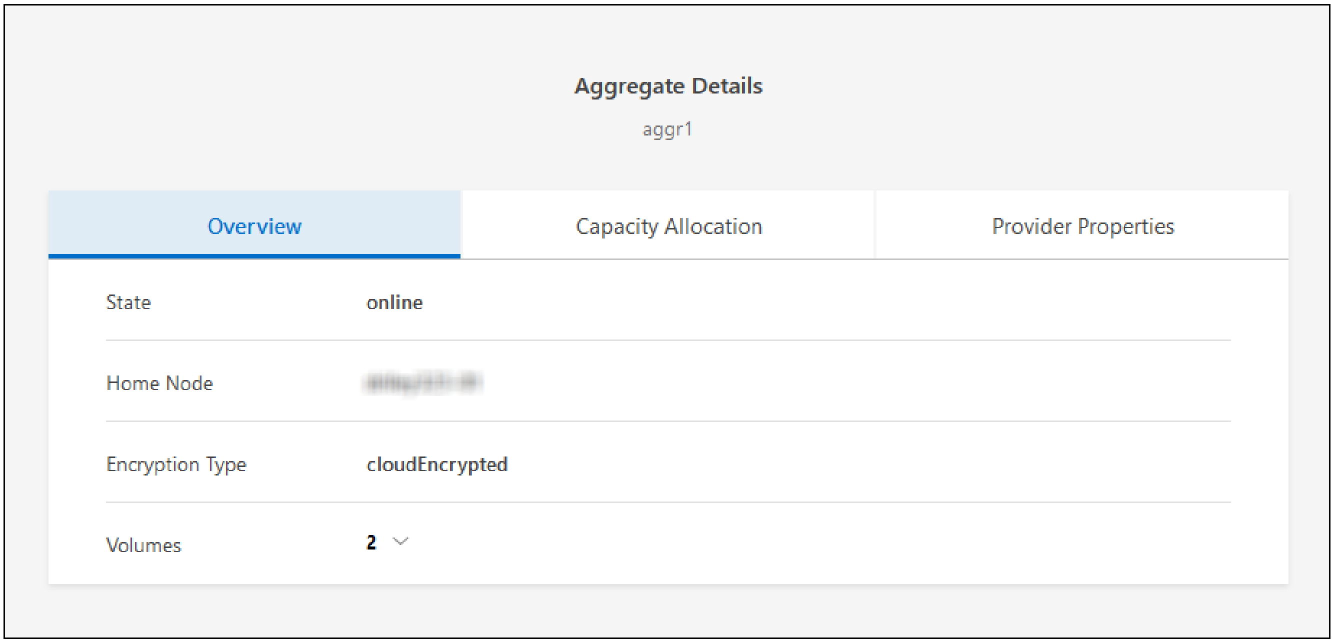
Aggregates for Cloud Volumes ONTAP must be online before you update the software. Aggregates should be online in most configurations, but if they are not, then you should bring them online.

About this task

These steps describe how to use ONTAP System Manager for version 9.3 and later.

Steps

1. On the Cloud Volumes ONTAP system, click the **Aggregates** tab.
2. On the required aggregate tile, click the ••• icon, and then select **View Aggregate details**.



3. If the aggregate is offline, use ONTAP System Manager to bring the aggregate online:
   a. Click **Storage > Aggregates & Disks > Aggregates**.
   b. Select the aggregate, and then click **More Actions > Status > Online**.

Verify that all LIFs are on home ports

Before you upgrade, all LIFs must be on home ports. Refer to the ONTAP documentation to verify that all LIFs are on home ports.

If an upgrade failure error occurs, consult the Knowledge Base (KB) article Cloud Volumes ONTAP upgrade fails.

Upgrade Cloud Volumes ONTAP

The Console notifies you when a new version is available for upgrade. You can start the upgrade process from this notification. For more information, see Upgrade from Console notifications.

Another way to perform software upgrades by using an image on an external URL. This option is helpful if the Console can't access the S3 bucket to upgrade the software or if you were provided with a patch. For more information, see Upgrade from an image available at a URL.

Upgrade from Console notifications

The Console displays a notification in Cloud Volumes ONTAP working environments when a new version of Cloud Volumes ONTAP is available:

> ⓘ Before you can upgrade Cloud Volumes ONTAP through the notifications, you must have a NetApp Support Site account.

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.

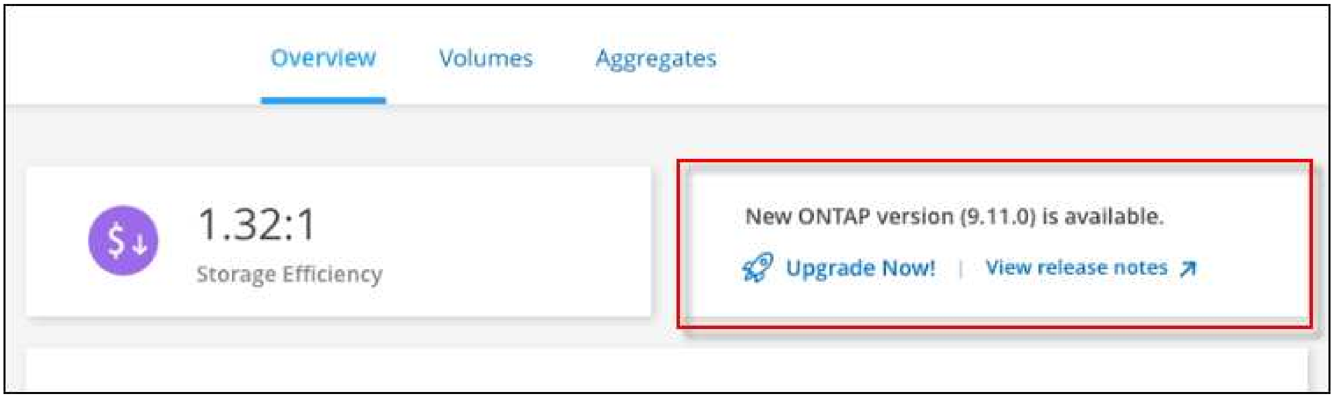
Before you begin

Operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.

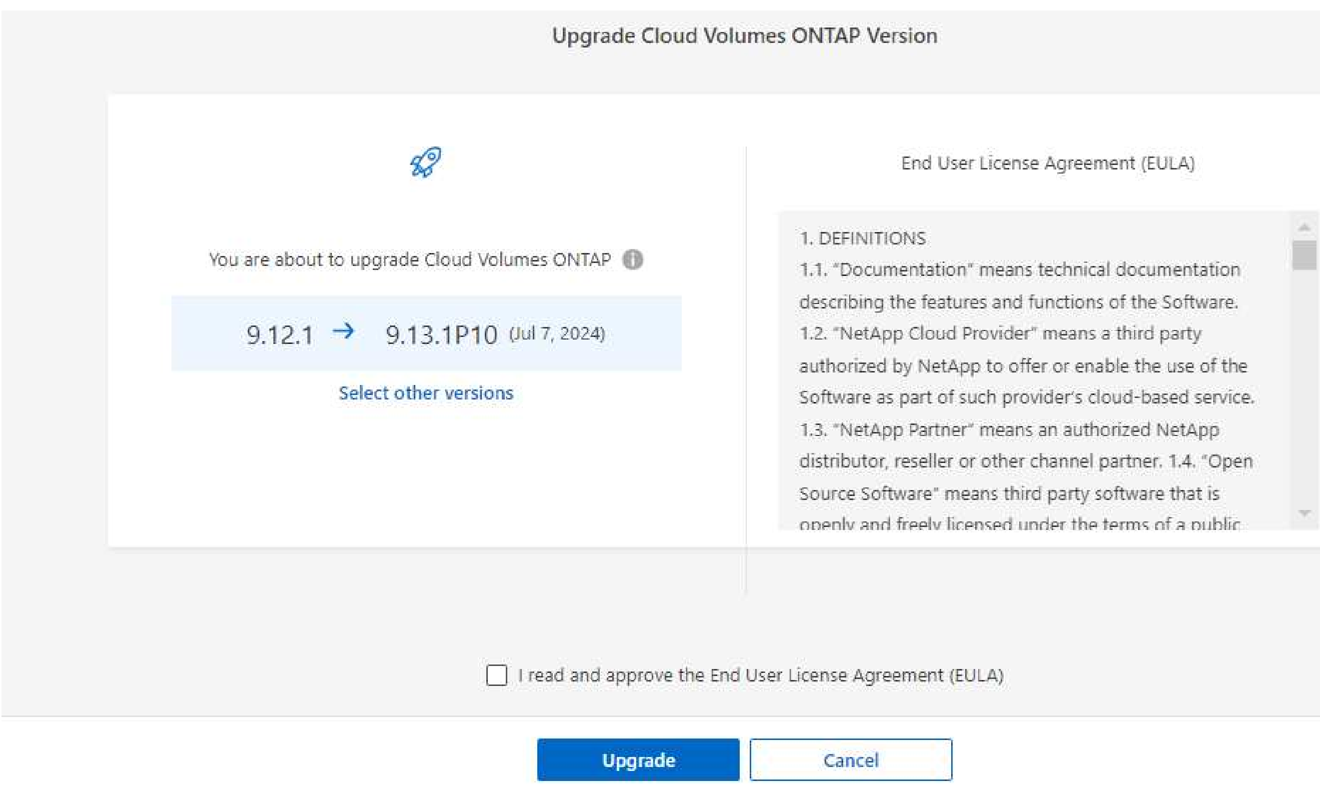
Steps

1. From the left navigation menu, select **Storage > Management**.
2. Select a Cloud Volumes ONTAP system.

   A notification appears in the Overview tab if a new version is available:

3. If you want to upgrade the installed version of Cloud Volumes ONTAP, click **Upgrade Now!** By default, you see the latest, compatible version for upgrade.

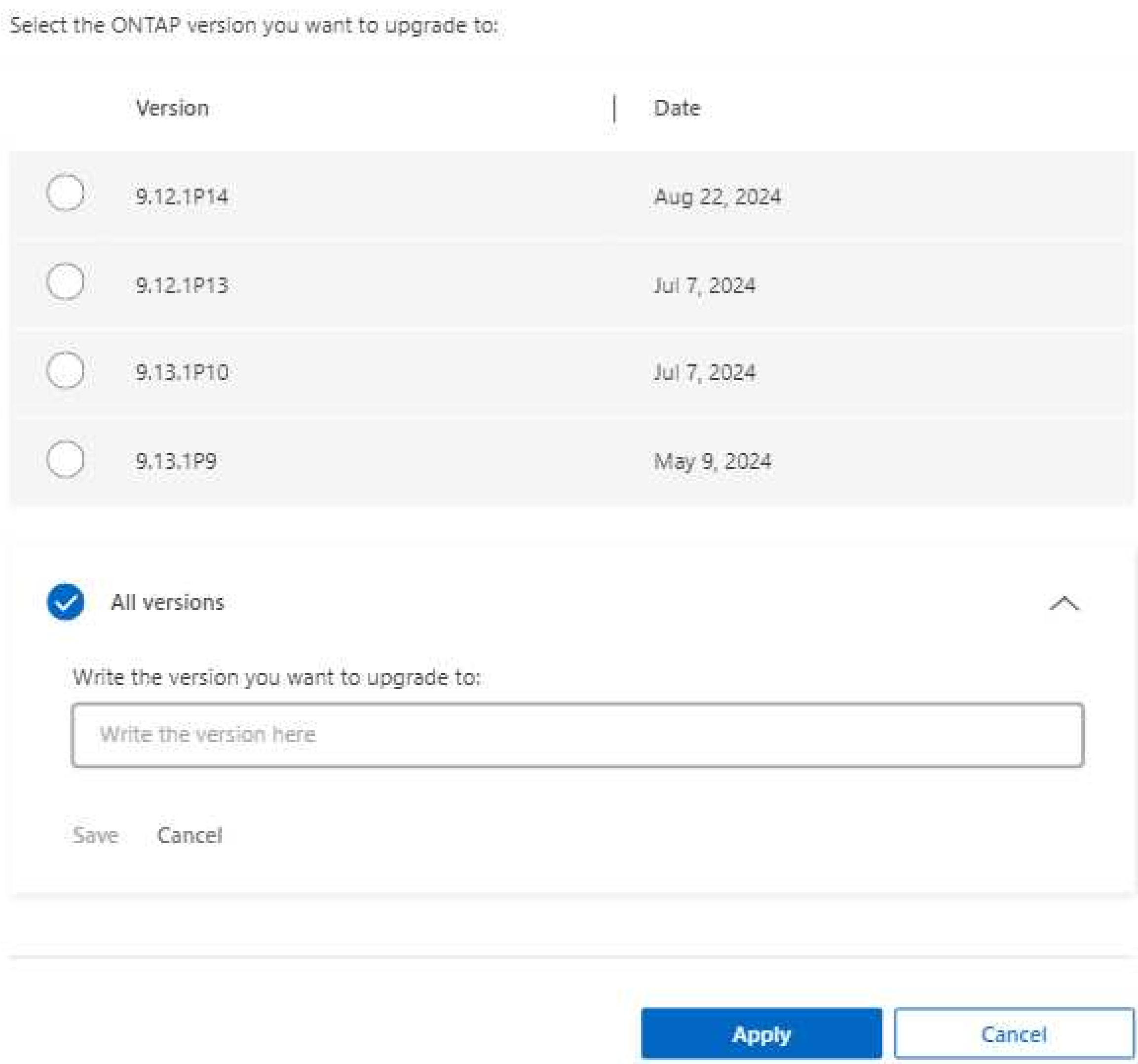
   

   If you want to upgrade to another version, click **Select other versions**. You see the latest Cloud Volumes

ONTAP versions listed that are also compatible with the installed version on your system.
For example, the installed version on your system is 9.12.1P3, and the following compatible versions are available:

   - 9.12.1P4 to 9.12.1P14
   - 9.13.1 and 9.13.1P1
     You see 9.13.1P1 as the default version for upgrade, and 9.12.1P13, 9.13.1P14, 9.13.1, and 9.13.1P1 as the other available versions.

4. Optionally, you can click **All versions** to enter another version that you want to upgrade to (say, the next patch of the installed version). For a compatible upgrade path of your current Cloud Volumes ONTAP version, refer to Supported upgrade paths.
5. Click **Save**, and then **Apply**.



6. In the Upgrade Cloud Volumes ONTAP page, read the EULA, and then select **I read and approve the EULA**.
7. Select **Upgrade**.
8. To view the progress, on the Cloud Volumes ONTAP system, select **Audit**.

Result

The Console starts the software upgrade. You can perform actions on the system when 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 Console agent or on an HTTP server and then initiate the software upgrade from the Console. You might use this option if the Console can't access the S3 bucket to upgrade the software.

Before you begin

- 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 the Console.

  Go to the NetApp Knowledge Base to view step-by-step instructions:

  NetApp KB: How to configure the Console as an HTTPS server to host upgrade images

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 Console agent or on an HTTP server from which the file will be served.

   Two paths are available. The correct path depends on your Console agent version.

   - `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
   - `/opt/application/netapp/cloudmanager/ontap/images/`

5. On the system, click the ••• icon, and then click **Update Cloud Volumes ONTAP**.
6. On the Update Cloud Volumes ONTAP version page, enter the URL, and then click **Change Image**.

   If you copied the software image to the Console agent in the path shown above, you would enter the following URL:

   http://<Console_agent_private-IP-address>/ontap/images/<image-file-name>

In the URL, **image-file-name** must follow the format "cot.image.9.13.1P2.tgz".

7. Click **Proceed** to confirm.

Result

The Console starts the software update. You can perform actions on the system once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

Fix download failures when using a Google Cloud NAT gateway

The Console agent automatically downloads software updates for Cloud Volumes ONTAP. The download can fail if your configuration uses a Google Cloud NAT gateway. You can correct this issue by limiting the number of parts that the software image is divided into. You must use the APIs to complete this step.

Step

1. Submit a PUT request to `/occm/`config with the following JSON as body:

```
{
  "maxDownloadSessions": 32
}
```

The value for *maxDownloadSessions* can be 1 or any integer greater than 1. If the value is 1, then the downloaded image will not be divided.

Note that 32 is an example value. The value that you should use depends on your NAT configuration and the number of sessions that you can have simultaneously.

Learn more about the /occm/config API call.

Register Cloud Volumes ONTAP pay-as-you-go systems

Support from NetApp is included with Cloud Volumes ONTAP pay-as-you-go (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.

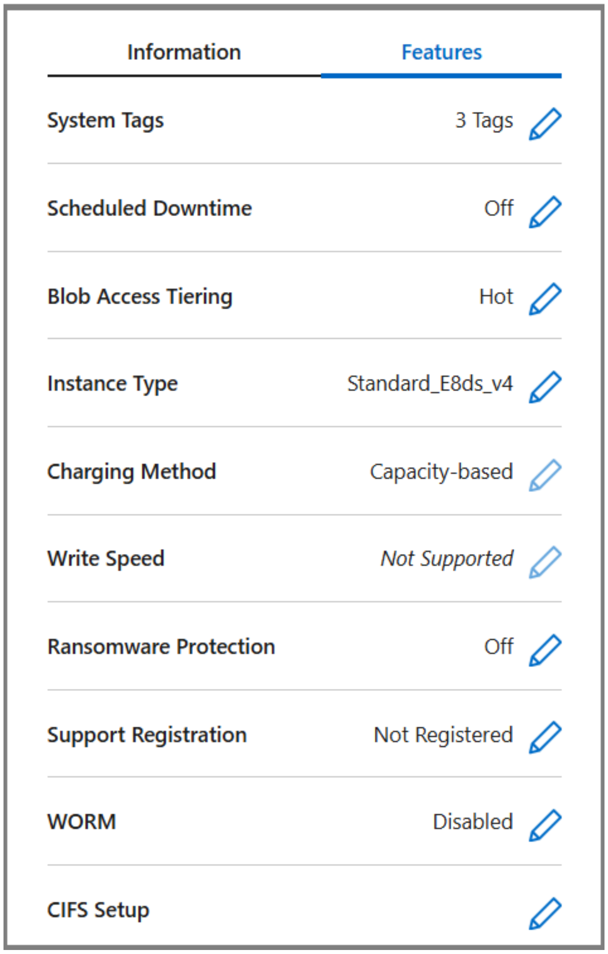
A system that isn't registered for support will still receive the software update notifications that appear in the NetApp Console when a new version is available. But you will need to register the system before you can upgrade the software.

Steps

1. If you have not yet added your NetApp Support Site account to the Console, go to **Account Settings** and add it now.

   Learn how to add NetApp Support Site accounts.

2. On the **Systems** page, double-click the name of the system you want to register..
3. On the Overview tab, click the Features panel and then click the pencil icon next to **Support Registration**.



4. Select a NetApp Support Site account and click **Register**.

Result

The system is registered with NetApp.

Convert a Cloud Volumes ONTAP node-based license to a capacity-based license

After the end of availability (EOA) of your node-based licenses, you should transition to capacity-based licensing by using the license conversion tool in the NetApp Console.

For annual or longer-term commitments, NetApp recommends that you contact your NetApp representative prior to the EOA date (11 November, 2024) or license expiration date to ensure that the prerequisites for the transition are in place. If you don't have a long-term contract for a Cloud Volumes ONTAP node and run your system against an on-demand pay-as-you-go (PAYGO) subscription, it is important to plan your conversion before the end of support (EOS) on 31 December, 2024. In both the cases, you should ensure that your system fulfills the requirements before you use the license conversion tool in the NetApp Console for a seamless transition.

For information about the EOA and EOS, refer to End of availability of node-based licenses.

About this task

- When you use the license conversion tool, the transition from node-based to capacity-based licensing model is carried out in place and online that eliminates the need for any data migration or provisioning of additional cloud resources.
- It is a non-disruptive operation, and no service disruption or application downtime occurs.
- The account and application data in your Cloud Volumes ONTAP system remains intact.
- The underlying cloud resources remain unaffected post conversion.
- The license conversion tool supports all deployment types, such as single node, high availability (HA) in single availability zone (AZ), HA in multiple AZ, bring your own license (BYOL), and PAYGO.
- The tool supports all node-based licenses as the source and all capacity-based licenses as the destination. For example, if you have a PAYGO Standard node-based license, you can convert it to any capacity-based license purchased through the marketplace. NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP.
- The conversion is supported for all cloud providers, AWS, Azure, and Google Cloud.
- Post conversion, the serial number of the node-based license will be replaced by a capacity-based format. This is done as a part of the conversion, and is reflected on your NetApp Support Site (NSS) account.
- When you transition to the capacity-based model, your data continues to be retained in the same location as the node-based licensing. This approach guarantees no disruption in data placement, and upholds data sovereignty principles throughout the transition.

Before your begin

- You should have an NSS account with customer access or administrator access.
- Your NSS account should be registered with the user credentials you used for accessing the Console.
- The Cloud Volumes ONTAP system should be linked to the NSS account with customer access or administrator access.
- You should have a valid capacity-based license in place, either a BYOL license or marketplace subscription.
- A capacity-based license should be available in your account. This license can be a marketplace subscription or a BYOL/private offer package available under **Licenses and subscriptions** in the Console.
- Understand the following criteria before selecting a destination package:
  - If the account has a capacity-based BYOL license, the destination package selected should align with the account’s BYOL capacity-based licenses:
    - When `Professional` is selected as the destination package, the account should have a BYOL license with a Professional package:
    - When `Essentials` is selected as the destination package, the account should have a BYOL license with the Essentials package.
  - If the destination package does not align with the account’s BYOL license availability, it implies that the capacity-based license might not include the selected package. In this case, you will be charged through your marketplace subscription.
  - If there is no capacity-based BYOL license but only a marketplace subscription, you should ensure that the selected package is included in your capacity-based marketplace subscription.
  - If there is not enough capacity in your existing capacity-based license, and if you have a marketplace subscription to charge for the additional capacity usage, you will be charged for the additional capacity through your marketplace subscription.

◦ If there is not enough capacity in your existing capacity-based license, and you don't have a marketplace subscription to charge for the additional capacity usage, the conversion cannot occur. You should add a marketplace subscription to charge the additional capacity or extend the available capacity to your current license.

◦ If the destination package does not align with the account's BYOL license availability and also if there is not enough capacity in your existing capacity-based license, then you will be charged through your marketplace subscription.

> If any of these requirements is not fulfilled, the license conversion does not happen. In specific cases, the license might be converted, but cannot be used. Click the information icon to identify the issues and take corrective actions.

Steps

1. On the **Systems** page, double-click the name of the system for which you want to modify the license type.
2. On the Overview tab, click the Features panel.
3. Check the pencil icon next to **Charging method**. If the charging method for your system is `Node Based`, you can convert it to by-capacity charging.

   > The icon is disabled if your Cloud Volumes ONTAP system is already charged by capacity, or if any of the requirements is not fulfilled.

4. On the **Convert Node-based licenses to Capacity-based** screen, verify the system name and source license details.
5. Select the destination package for converting the existing license:
   ◦ Essentials. The default value is `Essentials`.
   ◦ Professional
6. If you have a BYOL license, you can select the checkbox to delete the node-based license from the Console after the conversion is complete. If the conversion is still in progress, selecting this checkbox will not remove the license from the Console. This option is not available for marketplace subscriptions.
7. Select the check box to confirm that you understand the implications of the change, and then click **Proceed**.

After you finish

View the new license serial number and verify the changes in the **Licenses and subscriptions** menu of the Console.

Pricing in different hyperscalars

For details on pricing, go to the NetApp Console website.

For information about private offers in specific hyperscalars, write to:

- AWS - awspo@netapp.com
- Azure - azurepo@netapp.com
- Google Cloud - gcppo@netapp.com

Start and stop a Cloud Volumes ONTAP system

You can stop and start Cloud Volumes ONTAP from the NetApp Console 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 the Console 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, the Console postpones the shutdown if an active data transfer is in progress.

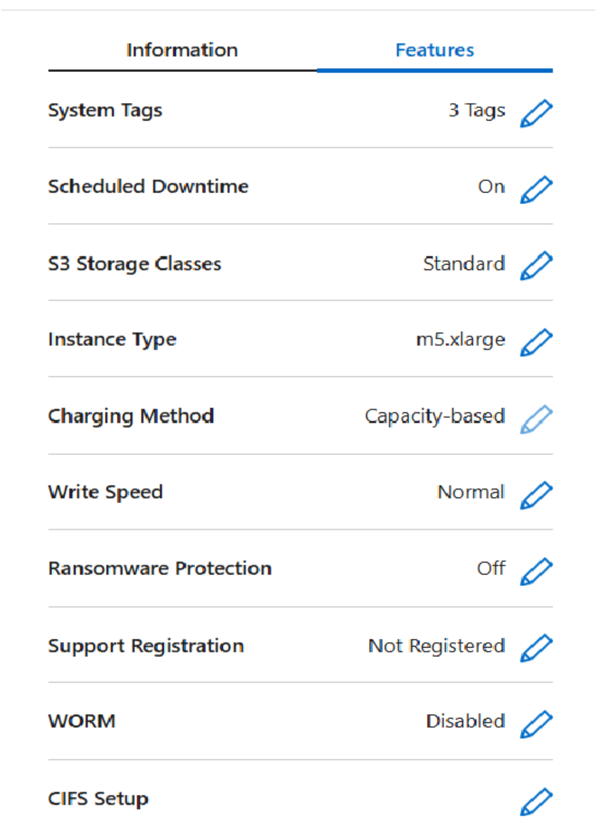
  It shuts down the system after the transfer is complete.

- 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

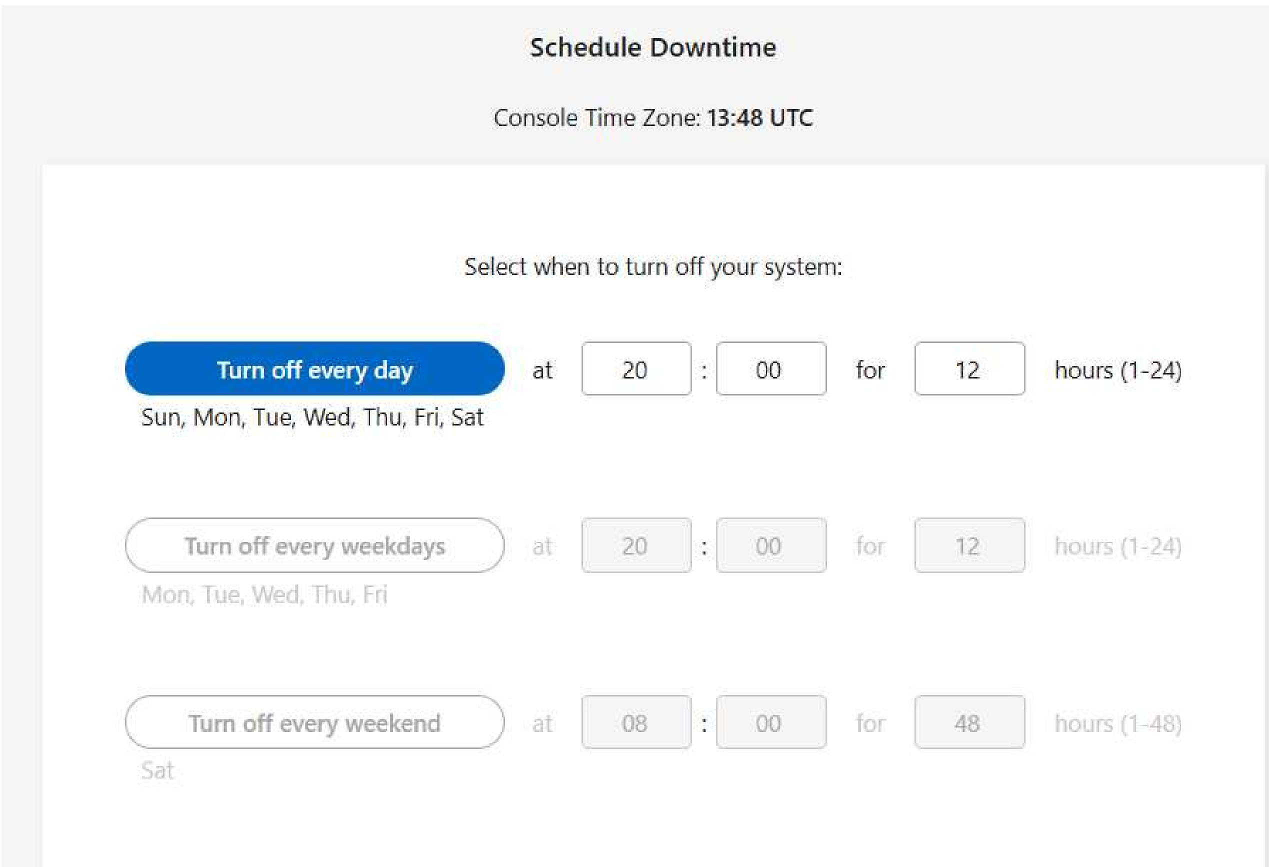
1. On the **Systems** page, double-click the Cloud Volumes ONTAP system.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Scheduled Downtime**.



3. 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 the Console to shut down the system every Saturday at 20:00 P.M. (8:00 PM) for 12 hours. The Console restarts the system every Monday at 12:00 a.m.



4. Click **Save**.

Result

The schedule is saved. The corresponding Scheduled Downtime line item under the Features panel displays 'On'.

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.

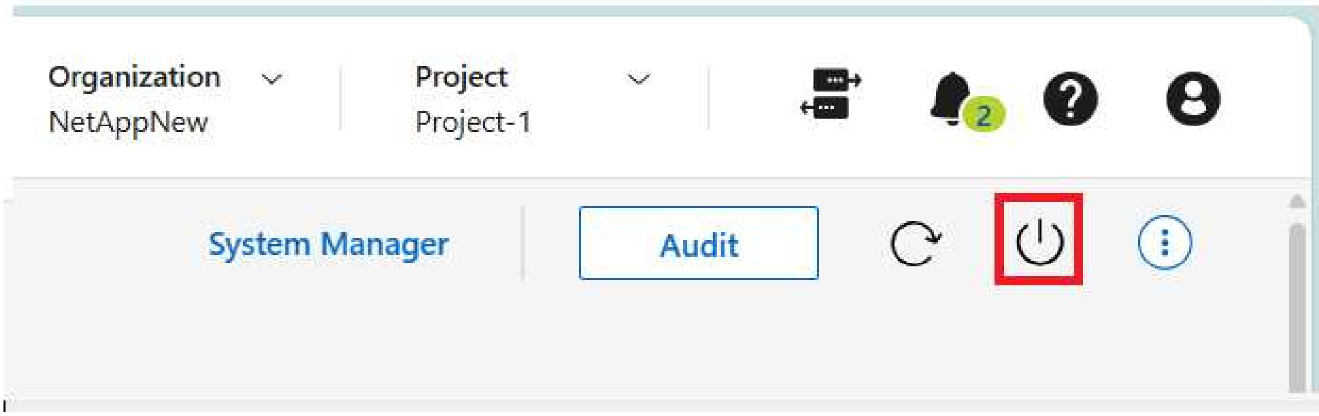
> ⓘ To reduce costs, the Console periodically deletes older snapshots of root and boot disks. Only the two most recent snapshots are retained for both the root and boot disks.

About this task

When you stop an HA pair, the Console shuts down both nodes.

Steps

1. From the system, 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 **Systems** page.

   > Snapshots are created automatically upon reboot.

Synchronize Cloud Volumes ONTAP system time using the NTP server

To ensure accurate time synchronization, you must set up a Network Time Protocol (NTP) server for your Cloud Volumes ONTAP systems. Make sure to configure an NTP server for your Cloud Volumes ONTAP systems on all cloud providers to maintain consistent time synchronization within your network.

> If you don't configure an NTP server, you might experience service disruptions and inaccurate time synchronization.

You can specify an NTP server using:

- The NetApp Console API.
- The ONTAP CLI command cluster time-service ntp server create.

Related links

- Knowledge base (KB) article: How does a CVO cluster use NTP?
- Prepare to use the API
- Cloud Volumes ONTAP workflows
- Get required identifiers
- Use the REST APIs for NetApp Console

Modify system write speed

You can choose a normal or high write speed for Cloud Volumes ONTAP in the NetApp Console. 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. On the **Systems** page, double-click the name of the system you configure to the write speed.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Write Speed**.
3. Select **Normal** or **High**.

   If you choose High, then you'll need to read the "I understand…" statement and confirm by checking the box.

   > The **High** write speed option is supported with Cloud Volumes ONTAP HA pairs in Google Cloud starting with version 9.13.0.

4. Click **Save**, review the confirmation message, and then click **Approve**.

Change the Cloud Volumes ONTAP cluster admin password

Cloud Volumes ONTAP includes a cluster admin account. You can change the password for this account from NetApp Console, if needed.

> You should not change the password for the admin account through ONTAP System Manager or the ONTAP CLI. The password will not be reflected in the Console. As a result, the Console cannot monitor the instance properly.

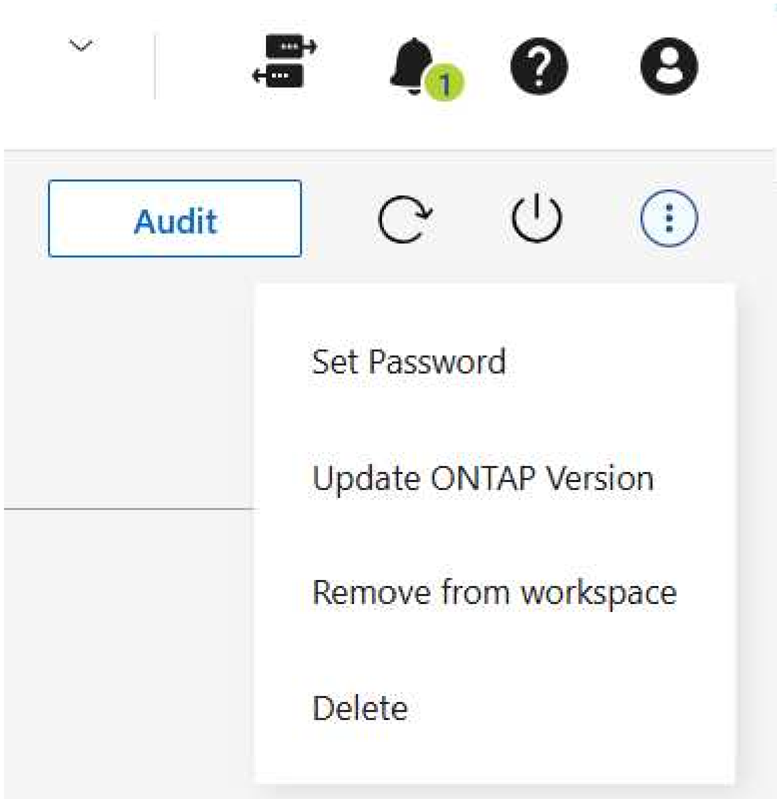
About this task

The password must observe a few rules. The new password:

- Shouldn't contain the word `admin`
- Must be between eight and 50 characters in length
- Must contain at least one English letter and one digit
- Shouldn't contain these special characters: `/ ( ) { } [ ] # : % " ? \`

Steps

1. On the **Systems** page, double-click the name of the Cloud Volumes ONTAP system.
2. On the upper right of the Console, click the ••• icon, and select **Set password**.



Add, remove, or delete systems

Add an existing Cloud Volumes ONTAP system to NetApp Console

You can discover and add existing Cloud Volumes ONTAP systems to the NetApp Console for centralized management. When you onboard a system with an account, the system is registered with that account. In environments with multiple accounts or organizations, you can only discover and manage systems registered with your Console login account.

When working with system registrations, ensure that all actions are performed within the same organization and account where the systems were originally onboarded. For example, you can move a Cloud Volumes ONTAP system to a new Console agent when the migration stays within the same organization.

> ! You can’t discover, view, or manage systems that are registered with a different account or organization.

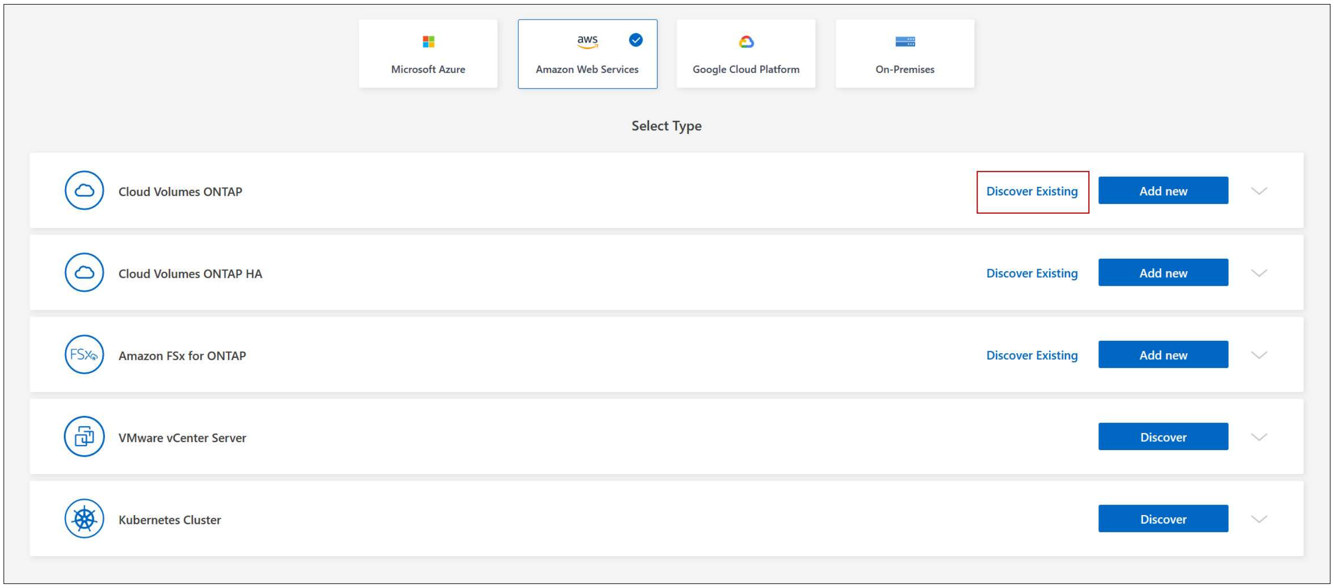
Before you begin

You must know the password for the Cloud Volumes ONTAP admin user account.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **System** page, click **Add System**.

3. Select the cloud provider in which the system resides.
4. Choose the type of Cloud Volumes ONTAP system to add.
5. Click the link to discover an existing system.



6. On the Region page, select a region. You can see the systems that are running in the selected region.

> Cloud Volumes ONTAP systems are represented as instances on this page. From the list, you can select only those instances that are registered with the current account.

7. On the Credentials page, enter the password for the Cloud Volumes ONTAP admin user, and then select **Go**.

Result

The Console adds the Cloud Volumes ONTAP systems to the **Systems** page.

Remove a Cloud Volumes ONTAP system from NetApp Console

You can remove a Cloud Volumes ONTAP system to move it to another system or to troubleshoot discovery issues.

About this task

Removing a Cloud Volumes ONTAP system removes it from the NetApp Console. It does not delete the Cloud Volumes ONTAP system. You can later rediscover the system if you need.

Steps

1. On the **Systems** page, double-click on the system you want to remove.
2. On the upper right of the Console, click the ••• icon, and select **Remove from workspace**.
3. In the **Remove from workspace** window, click **Remove**.

Result

The Console removes the system. Users can rediscover the deleted system from the **Systems** page at any time.

Delete a Cloud Volumes ONTAP system from NetApp Console

You should always delete Cloud Volumes ONTAP systems from the NetApp Console, rather than from your cloud provider's application. 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 Cloud Volumes ONTAP system from the Console to release the license.

When you delete a system, the Console terminates Cloud Volumes ONTAP instances and deletes disks and snapshots.

> Other resources, such as backups managed by NetApp Backup and Recovery, and instances for NetApp Data Classification, are not deleted when you delete a system. You'll need to manually delete them. If you don't, then you'll continue to incur charges for these resources.

When the Console 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 Backup and Recovery on the system, determine whether the backed up data is still required and then delete the backups, if necessary.

   Backup and Recovery is independent from Cloud Volumes ONTAP by design. Backup and Recovery 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 Data Classification on this system and no other systems use this service, then you need to delete the instance for the service.

   Learn more about the Data Classification instance.

3. Delete the Cloud Volumes ONTAP system.
   a. On the **Systems** page, double-click the name of the Cloud Volumes ONTAP system that you want to delete.
   b. On the upper right of the Console, click the ••• icon, and select **Delete**.
   c. Type the name of the system you want to delete, and then click **Delete**. It can take up to five minutes to delete a system.

> Backup and Recovery is free only for Cloud Volumes ONTAP Professional licenses. This free benefit does not apply to deleted environments. If backed up copies of the Cloud Volumes ONTAP environment are retained in a Backup and Recovery instance, you will be charged for the backed up copies until they are deleted.

AWS administration

Modify the EC2 instance type for a Cloud Volumes ONTAP system in AWS

You can choose from several instance or types when you launch Cloud Volumes ONTAP in AWS. You can change the instance 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 instance type can affect AWS 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.

  > The NetApp Console changes one node at a time by initiating takeover and waiting for give back. NetApp's Quality Assurance team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, some retries were observed on the I/O level, but the application layer overcame the rewiring of NFS/CIFS connections.

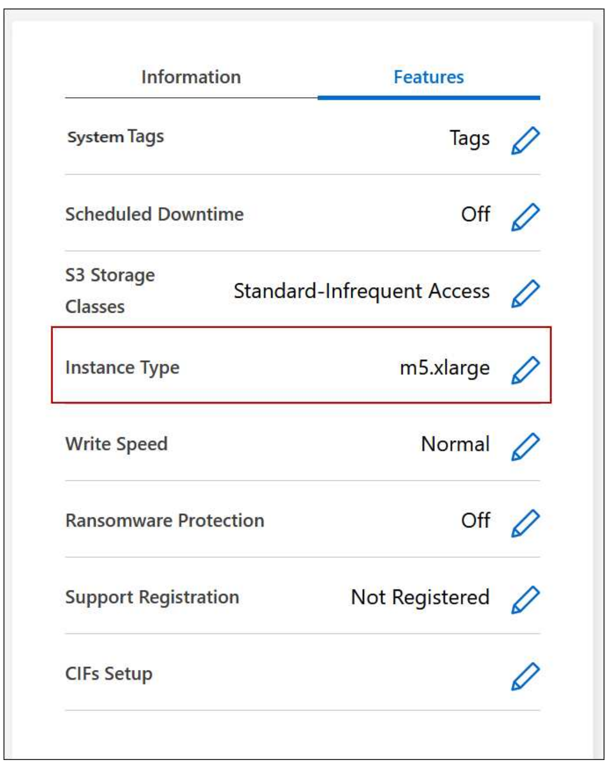
Reference

For a list of supported instance types in AWS, refer to Supported EC2 instances.

If you can't change the instance type from c4, m4, or r4 instances, refer to KB article "Converting an AWS Xen CVO instance to Nitro (KVM)".

Steps

1. On the **Systems** page, select the system.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Instance type**.



If you are using a node-based pay as you go (PAYGO) license, you can optionally choose a different license and instance type by clicking the pencil icon next to **License type**.

3. Choose an instance type, select the check box to confirm that you understand the implications of the change, and then click **Change**.

Result

Cloud Volumes ONTAP reboots with the new configuration.

Modify route tables for Cloud Volumes ONTAP HA pairs in multiple AWS AZs

You can modify the AWS route tables that include routes to the floating IP addresses for an HA pair that's deployed in multiple AWS Availability Zones (AZs). You might do this if new NFS or CIFS clients need to access an HA pair in AWS.

Steps

1. On the **Systems** page, select the system.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Route tables**.
3. Modify the list of selected route tables and then click **Save**.

Result

The NetApp Console sends an AWS request to modify the route tables.

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.

> NetApp Console changes one node at a time by initiating takeover and waiting for give back. NetApp's Quality Assurance team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, some retries were observed on the I/O level, but the application layer overcame the rewiring of NFS/CIFS connections.

Steps

1. On the **Systems** page, select the system.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **VM type**.

   If you are using a node-based pay-as-you-go (PAYGO) license, you can optionally choose a different license and VM type by clicking the pencil icon next to **License type**.

3. Select a VM type, select the check box to confirm that you understand the implications of the change, and then click **Change**.

Result

Cloud Volumes ONTAP reboots with the new configuration.

Override CIFS locks for Cloud Volumes ONTAP HA pairs in Azure

The organization or account admin can enable a setting in the NetApp Console 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.

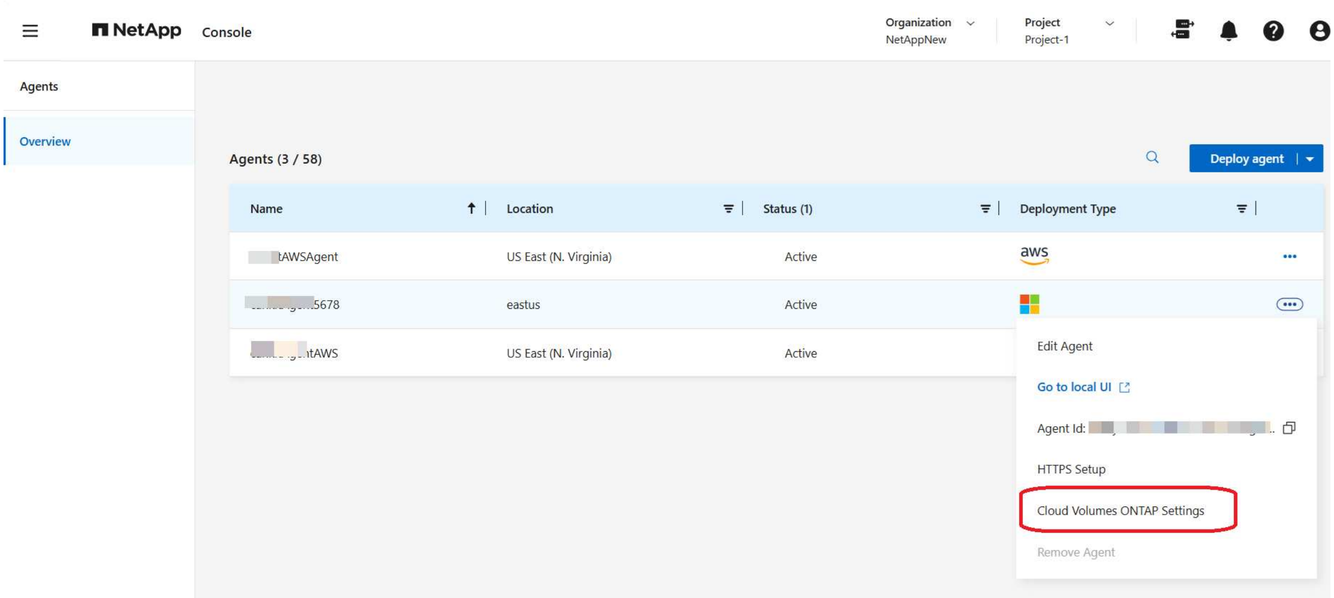
> This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

Before you begin

You need to create a Console agent before you can change the Console settings. Learn how.

Steps

1. From the left navigation pane, go to **Administration > Agents**.
2. Click the ••• icon for the Console agent that manages your Cloud Volumes ONTAP system.
3. Select **Cloud Volumes ONTAP Settings**.



4. Under **Azure**, click **Azure CIFS locks for Azure HA systems**.
5. Click the checkbox to enable the feature and then click **Save**.

Use an Azure Private Link or service endpoints for Cloud Volumes ONTAP systems

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, the NetApp Console 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, the Console 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 Console agent is deployed.

Disable Azure Private Links and use service endpoints instead

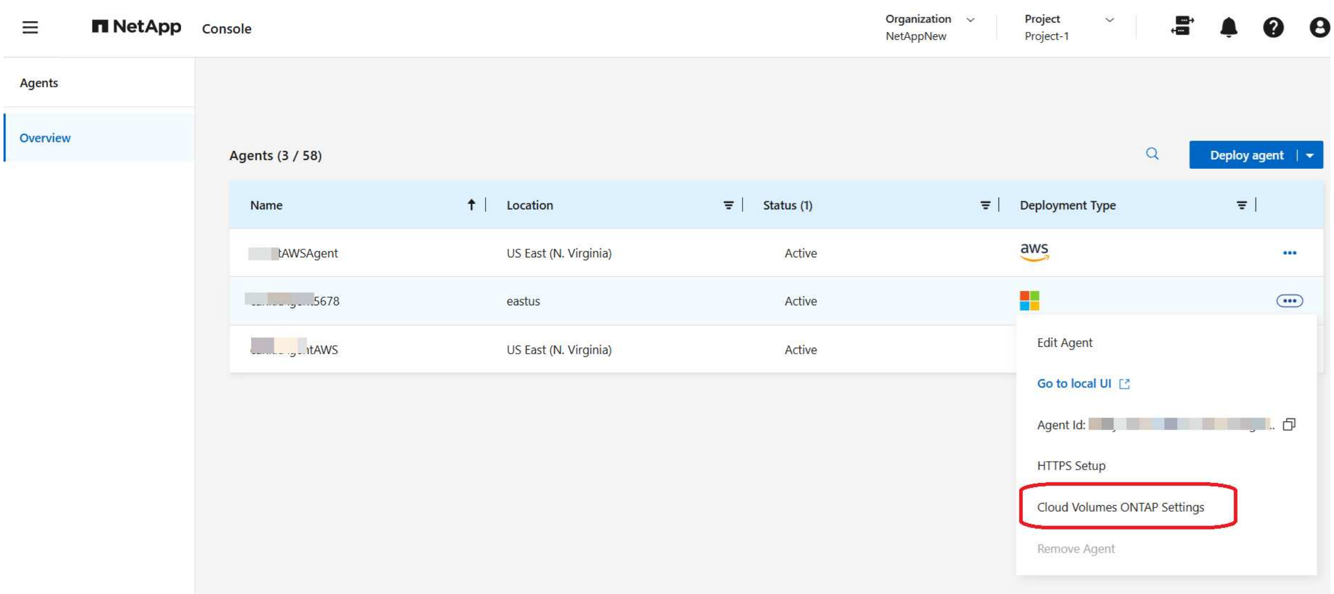
If required by your business, you can change a setting in the Console so that it configures Cloud Volumes ONTAP to use service endpoints instead of an Azure Private Link. Changing this setting applies to new Cloud Volumes ONTAP systems that you create. Service endpoints are only supported in Azure region pairs between the Console agent and Cloud Volumes ONTAP VNets.

The Console agent 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.

Steps

1. From the left navigation pane, go to **Administration > Agents**.

2. Click the icon for the Console agent that manages your Cloud Volumes ONTAP system.
3. Select **Cloud Volumes ONTAP Settings**.



4. Under **Azure**, click **Use Azure Private Link**.
5. Deselect **Private Link connection between Cloud Volumes ONTAP and storage accounts**.
6. Click **Save**.

After you finish

If you disabled Azure Private Links and the Console agent uses a proxy server, you must enable direct API traffic.

Learn how to enable direct API traffic on the Console agent

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. The Console manages Azure Private Links for you. But if you use an existing Azure Private DNS zone, then you'll need to edit a configuration file.

Requirement for custom DNS

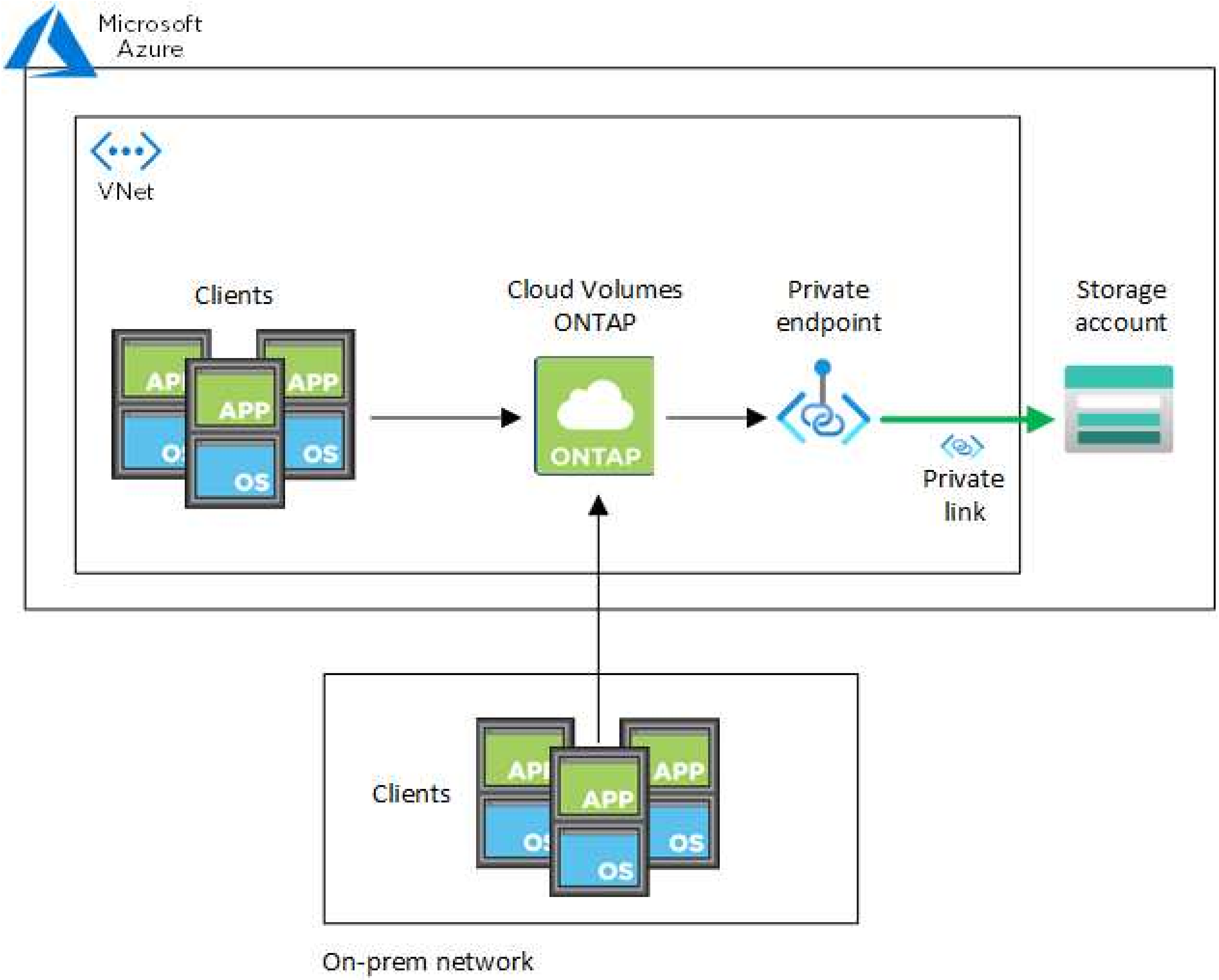
Optionally, if you work with custom DNS, you need to create a conditional forwarder to the Azure private DNS zone from your custom DNS servers. To learn more, refer to Azure's documentation on using a DNS forwarder.

How Private Link connections work

When the Console 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-premises network that has either a private VPN or ExpressRoute connection.



> If the Console agent and Cloud Volumes ONTAP systems are deployed in different VNets, then you must set up VNet peering between the VNet where the Console agent is deployed and the VNet where the Cloud Volumes ONTAP systems are deployed.

Provide details about your Azure Private DNS

If you use Azure Private DNS, then you need to modify a configuration file on each Console agent. Otherwise, the Console can't set 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 Console agent host and log in.
2. Navigate to the `/opt/application/netapp/cloudmanager/docker_occm/data` directory.
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,
   "create-private-dns-zone-link" : true
}
```

The `subscription` keyword is required only if the private DNS zone is in a different subscription than that of the Console agent.

4. Save the file and log off the Console agent.

   A reboot isn't required.

Enable rollback on failures

If the Console 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 system (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 the Console 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, the Console stops the action and rolls back all resources that were created as part of the action.

You can enable rollback through the API or by updating the app.conf file.

Enable rollback through the API

Step

1. Use the `PUT /occm/config` API call with the following request body:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

Enable rollback by updating app.conf

Steps

1. SSH to the host of the Console agent and log in.
2. Navigate to the following directory: /opt/application/netapp/cloudmanager/docker_occm/data
3. Edit app.conf by adding the following parameter and value:

```
"rollback-on-private-link-failure": true
```

4. Save the file and log off the Console agent.

A reboot isn't required.

Move an Azure resource group for Cloud Volumes ONTAP in Azure console

Cloud Volumes ONTAP supports Azure resource groups moves but the workflow happens in the Azure console only.

You can move a Cloud Volumes ONTAP system from one resource group to a different resource group in Azure within the same Azure subscription. Moving resource groups between different Azure subscriptions is not supported.

Steps

1. Remove the Cloud Volumes ONTAP system. Refer to Removing Cloud Volumes ONTAP systems.
2. Execute the resource group move in the Azure console.

   To complete the move, refer to Move resources to a new resource group or subscription in Microsoft Azure's documentation.

3. On the **Systems** page, discover the system.
4. Look for the new resource group in the information for the system.

Result

The system and its resources (VMs, disks, storage accounts, network interfaces, snapshots) are in the new resource group.

Segregate SnapMirror traffic in Azure

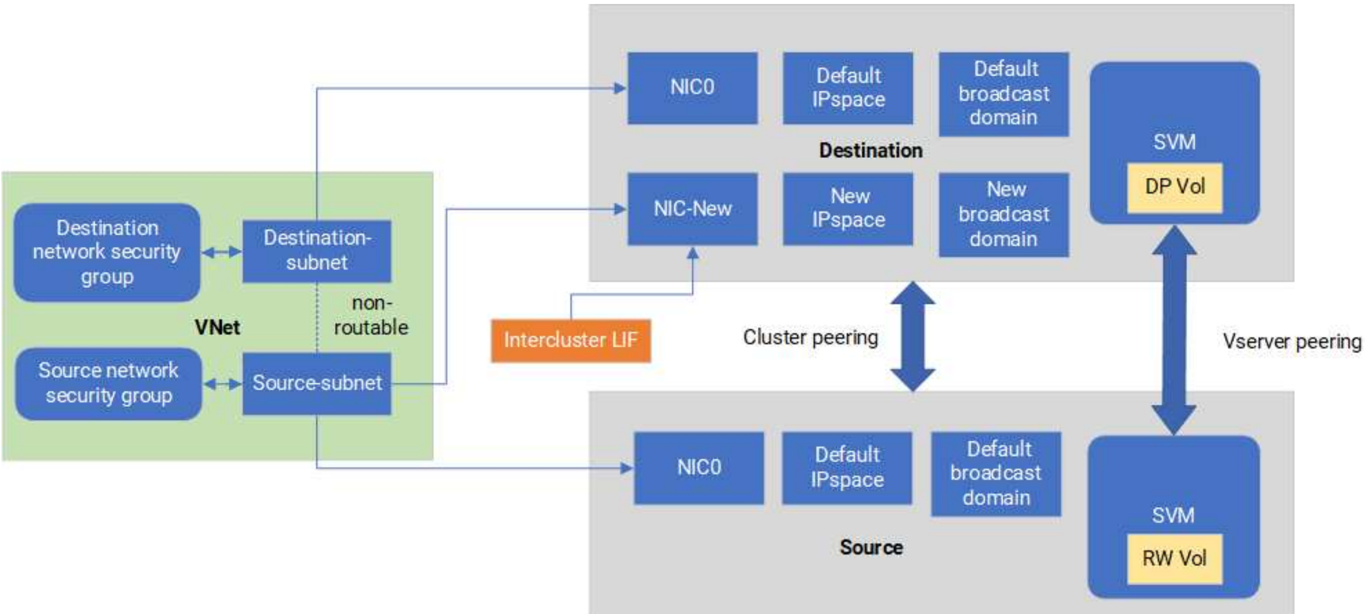
With Cloud Volumes ONTAP in Azure, you can segregate SnapMirror replication traffic from data and management traffic. To segregate SnapMirror replication traffic from your data traffic, you'll add a new network interface card (NIC), an associated intercluster LIF and a non-routable subnet.

About SnapMirror traffic segregation in Azure

By default, the NetApp Console configures all NICs and LIFs in a Cloud Volumes ONTAP deployment on the same subnet. In such configurations, SnapMirror replication traffic and data and management traffic use the same subnet. Segregating SnapMirror traffic leverages an additional subnet that isn't routable to the existing subnet used for data and management traffic.

Figure 1

The following diagrams show the segregation of SnapMirror replication traffic with an additional NIC, an associated intercluster LIF and a non-routable subnet in a single node deployment. An HA pair deployment differs slightly.



Before you begin

Review the following considerations:

- You can only add a single NIC to a Cloud Volumes ONTAP single node or HA-pair deployment (VM instance) for SnapMirror traffic segregation.
- To add a new NIC, the VM instance type you deploy must have an unused NIC.
- The source and destination clusters should have access to the same Virtual Network (VNet). The destination cluster is a Cloud Volumes ONTAP system in Azure. The source cluster can be a Cloud Volumes ONTAP system in Azure or an ONTAP system.

Step 1: Create an additional NIC and attach to the destination VM

This section provides instructions for how to create an additional NIC and attach it to the destination VM. The destination VM is the single node or HA-pair system in Cloud Volumes ONTAP in Azure where you want to set up your additional NIC.

Steps

1. In the ONTAP CLI, stop the node.

```
dest::> halt -node <dest_node-vm>
```

2. In the Azure portal, check that the VM (node) status is stopped.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Use the Bash environment in Azure Cloud Shell to stop the node.

   a. Stop the node.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. Deallocate the node.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-
vm>
```

4. Configure network security group rules to make the two subnets (source cluster subnet and destination cluster subnet) non-routable to each other.
   a. Create the new NIC on the destination VM.
   b. Look up the subnet ID for the source cluster subnet.

   ```
   az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet
   -name <vnet> --query id
   ```

   c. Create the new NIC on the destination VM with the subnet ID for the source cluster subnet. Here you enter the name for the new NIC.

   ```
   az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new>
   --subnet <id_from_prev_command> --accelerated-networking true
   ```

   d. Save the privateIPAddress. This IP address, <new_added_nic_primary_addr>, is used to create an intercluster LIF in broadcast domain, intercluster LIF for the new NIC.
5. Attach the new NIC to the VM.

   ```
   az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics
   <dest_node-vm-nic-new>
   ```

6. Start the VM (node).

   ```
   az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
   ```

7. In the Azure portal, go to **Networking** and confirm that the new NIC, e.g. nic-new, exists and accelerated networking is enabled.

   ```
   az network nic list --resource-group azure-59806175-60147103-azure-rg
   --query "[].{NIC: name, VM: virtualMachine.id}"
   ```

For HA-pair deployments, repeat the steps for the partner node.

Step 2: Create a new IPspace, broadcast domain, and intercluster LIF for the new NIC

A separate IPspace for intercluster LIFs provides logical separation between networking functionality for replication between clusters.

Use the ONTAP CLI for the following steps.

Steps

1. Create the new IPspace (new_ipspace).

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. Create a broadcast domain on the new IPspace (new_ipspace) and add the nic-new port.

```
dest::> network port show
```

3. For single-node systems, the newly added port is *e0b*. For HA-pair deployments with managed disks, the newly added port is *e0d*. For HA-pair deployments with page blobs, the newly added port is *e0e*. Use the node name not the VM name. Find the node name by running `node show`.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. Create an intercluster LIF on the new broadcast-domain (new_bd) and on the new NIC (nic-new).

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. Verify creation of the new intercluster LIF.

```
dest::> net int show
```

For HA-pair deployments, repeat the steps for the partner node.

Step 3: Verify cluster peering between the source and destination systems

This section provides instructions for how to verify peering between the source and destination systems.

Use the ONTAP CLI for the following steps.

Steps

1. Verify that the intercluster LIF of the destination cluster can ping the intercluster LIF of the source cluster. Because the destination cluster executes this command, the destination IP address is the intercluster LIF

IP address on the source.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. Verify that the intercluster LIF of the source cluster can ping the intercluster LIF of the destination cluster. The destination is the IP address of the new NIC created on the destination.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

For HA-pair deployments, repeat the steps for the partner node.

Step 4: Create SVM peering between the source and destination system

This section provides instructions for how to create SVM peering between the source and destination system.

Use the ONTAP CLI for the following steps.

Steps

1. Create cluster peering on the destination using the source intercluster LIF IP address as the `-peer -addrs`. For HA pairs, list the source intercluster LIF IP address for both nodes as the `-peer-addrs`.

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. Enter and confirm the passphrase.
3. Create cluster peering on the source using the destination cluster LIF IP address as the `peer-addrs`. For HA pairs, list the destination intercluster LIF IP address for both nodes as the `-peer-addrs`.

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. Enter and confirm the passphrase.
5. Check that the cluster peered.

```
src::> cluster peer show
```

   Successful peering shows **Available** in the availability field.

6. Create SVM peering on the destination. Both source and destination SVMs should be data SVMs.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. Accept SVM peering.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. Check that the SVM peered.

```
dest::> vserver peer show
```

Peer state shows **`peered`** and peering applications shows **`snapmirror`**.

Step 5: Create a SnapMirror replication relationship between the source and destination system

This section provides instructions for how to create a SnapMirror replication relationship between the source and destination system.

To move an existing SnapMirror replication relationship, you must first break the existing SnapMirror replication relationship before you create a new SnapMirror replication relationship.

Use the ONTAP CLI for the following steps.

Steps

1. Create a data protected volume on the destination SVM.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. Create the SnapMirror replication relationship on the destination which includes the SnapMirror policy and schedule for the replication.

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. Initialize the SnapMirror replication relationship on the destination.

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. In the ONTAP CLI, validate the SnapMirror relationship status by running the following command:

```
dest::> snapmirror show
```

The relationship status is `Snapmirrored` and the health of the relationship is `true`.

5. Optional: In the ONTAP CLI, run the following command to view the actions history for the SnapMirror relationship.

```
dest::> snapmirror show-history
```

Optionally, you can mount the source and destination volumes, write a file to the source, and verify the volume is replicating to the destination.

Google Cloud administration

Change the Google Cloud machine type for Cloud Volumes ONTAP

You can choose from several machine types when you launch Cloud Volumes ONTAP in Google Cloud. You can change the instance or machine 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 machine type can affect Google Cloud service charges.
- The operation restarts Cloud Volumes ONTAP.

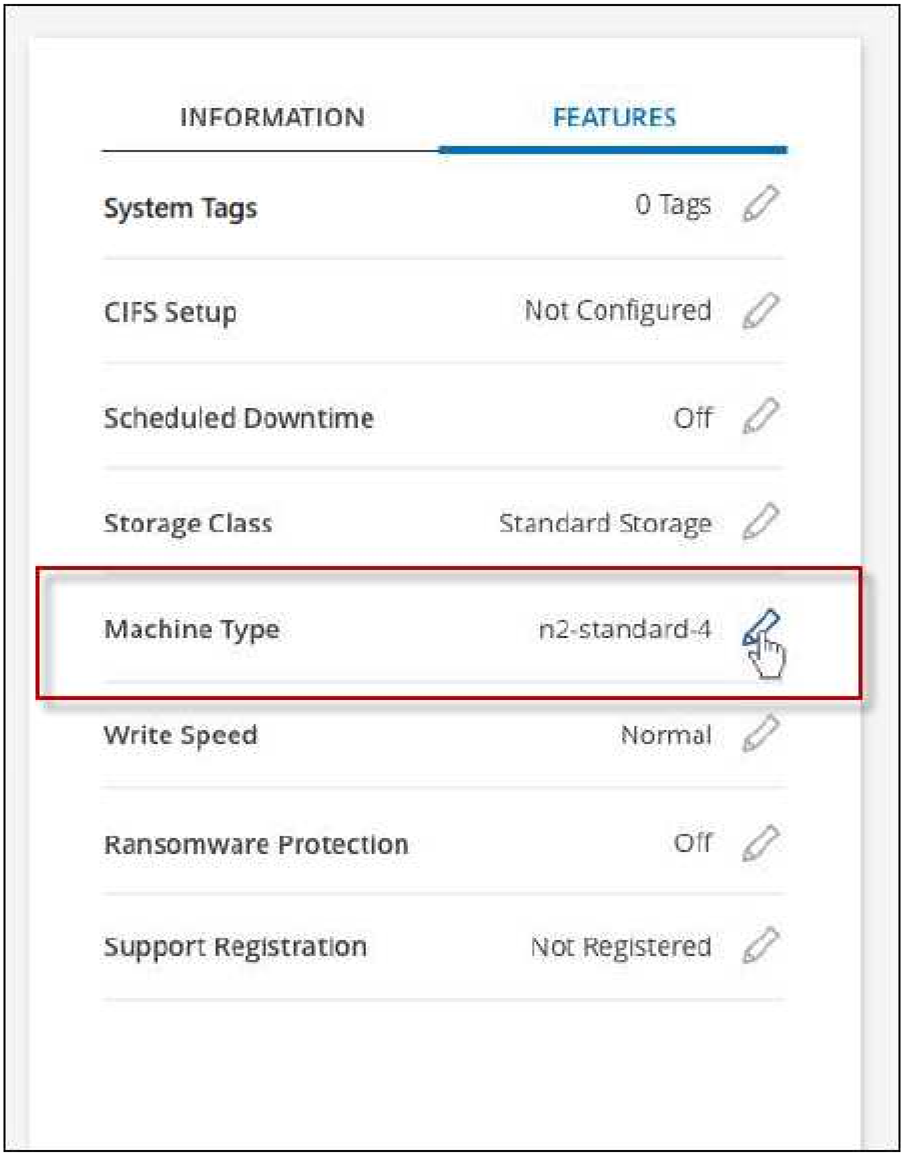
  For single-node systems, I/O is interrupted.

  For HA pairs, the change is nondisruptive. HA pairs continue to serve data.

  > The NetApp Console changes one node at a time by initiating takeover and waiting for give back. NetApp's Quality Assurance team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, some retries were observed on the I/O level, but the application layer overcame the rewiring of NFS/CIFS connections.

Steps

1. On the **Systems** page, select the system.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Machine type**.



If you are using a node-based pay-as-you-go (PAYGO) license, you can optionally choose a different license and machine type by clicking the pencil icon next to **License type**.

1. Choose an machine type, select the check box to confirm that you understand the implications of the change, and then click **Change**.

Result

Cloud Volumes ONTAP reboots with the new configuration.

Convert existing Cloud Volumes ONTAP deployments to Infrastructure Manager

Beginning on February 09, 2026, new Cloud Volumes ONTAP deployments in Google Cloud can use Google Cloud Infrastructure Manager. Google is about to deprecate Google Cloud Deployment Manager in favor of Infrastructure Manager. Therefore, you need to manually run a transition tool to convert your existing Cloud Volumes ONTAP deployments from Deployment Manager to Infrastructure Manager. This is a one-time process, after which your systems will automatically start using Infrastructure Manager.

About this task

The transition tool is available in the NetApp Support site, and creates the following artifacts:

- Terraform artifacts, saved in `conversion_output/deployment_name`.
- Summary of the conversion, saved in `conversion_output/batch_summary_<deployment_name>_<timestamp>.json`.
- Debug logs, saved in the `<gcp project number>-<region>-blueprint-config/<cvo name>` directory. You need these logs for troubleshooting. The `<gcp project number>-<region>-blueprint-config` bucket stores the Terraform logs.

> Cloud Volumes ONTAP systems using Infrastructure Manager store data and records in Google Cloud Storage buckets. You might incur extra costs for these buckets, but do not edit or delete the buckets or their content:
>
> - `gs://netapp-cvo-infrastructure-manager-<project id>`: for ONTAP versions and SVM Terraform Templates used for new Cloud Volumes ONTAP deployments. Inside this, the `dm-to-im-convert` bucket contains the Cloud Volumes ONTAP Terraform files.
> - `<gcp project number>-<region>-blueprint-config`: for storing Google Cloud Terraform artifacts.

Before you begin

- Ensure that your Cloud Volumes ONTAP system is 9.16.1 or later.
- Ensure that none of the Cloud Volumes ONTAP resources or their properties have been manually edited from the Google Cloud Console.
- Ensure that the Google Cloud APIs are enabled. Refer to Enable Google Cloud APIs. Ensure that along with the other APIs, you enable the Google Cloud Quotas API.
- Verify that the NetApp Console agent's service account has all required permissions. Refer to Google Cloud permissions for the Console agent.

  For private mode deployments, ensure these additional prerequisites:

  - Ensure that you have the latest Console agent version. Download the product installer from the NetApp Support Site and then manually install the agent on your host so that the agent can use Infrastructure Manager APIs.
  - If you are running the tool in a private mode, ensure that along with the other APIs, you have enabled the Cloud Build API. Enable Google Cloud APIs.
  - Ensure that you have completed the network configurations and created the worker pool for private mode deployments. Refer to Infrastructure Manager configuration for private mode deployments.

- The conversion tool uses the following domains. Enable them on port 443 in your network:

Domain	Port	Protocol	Direction	Purpose
cloudresourcemanager.googleapis.com	443	TCP	EGRESS	Project validation

Domain	Port	Protocol	Direction	Purpose
deploymentmanager.googleapis.com	443	TCP	EGRESS	Deployment discovery
config.googleapis.com	443	TCP	EGRESS	Infrastructure Manager API
storage.googleapis.com	443	TCP	EGRESS	GCS bucket operations
iam.googleapis.com	443	TCP	EGRESS	Service account validation
compute.googleapis.com	443	TCP	EGRESS	Compute API calls used by Google Cloud and Terraform Import and Plan
cloudbuild.googleapis.com	443	TCP	EGRESS	Build operations only required for private mode
openidconnect.googleapis.com	443	TCP	EGRESS	Authentication
oauth2.googleapis.com	443	TCP	EGRESS	OAuth2 token exchange
registry.terraform.io	443	TCP	EGRESS	Terraform provider registry
releases.hashicorp.com	443	TCP	EGRESS	Terraform binary downloads
apt.releases.hashicorp.com	443	TCP	EGRESS	HashiCorp APT repository
us-central1-docker.pkg.dev	443	TCP	EGRESS	GCP Artifact Registry
metadata.google.internal	80	HTTP	Internal	VM metadata & auth tokens
pypi.org	443	TCP	EGRESS	Python package index
files.pythonhosted.org	443	TCP	EGRESS	Python package downloads
checkpoint-api.hashicorp.com	443	TCP	EGRESS	Terraform version check
download.docker.com	443	TCP	EGRESS	Docker APT repository
security.ubuntu.com	80/443	TCP	EGRESS	Ubuntu security updates
*.gce.archive.ubuntu.com	80	TCP	EGRESS	Ubuntu package mirror

Prepare the environment for running the tool

Run these steps before running the tool.

Steps

1. Create a role and attach it to a service account:
   a. Create a YAML file with the following permissions:

```
title: NetApp Dm TO IM Convert Solution
description: Permissions for the service account associated with the
VM where the tool will run.
stage: GA
includedPermissions:
- compute.addresses.get
- compute.disks.get
- compute.forwardingRules.get
- compute.healthChecks.get
- compute.instanceGroups.get
- compute.instances.get
- compute.regionBackendServices.get
- config.deployments.create
- config.deployments.get
- config.deployments.getLock
- config.deployments.lock
- config.deployments.unlock
- config.deployments.update
- config.deployments.delete
- config.deployments.updateState
- config.operations.get
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- iam.serviceAccounts.get
- storage.buckets.create
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list
```

   Include additional permission for private mode deployments

   If you are running the tool in a private mode, add the `cloudbuild.workerpools.get` permission also to the YAML file.

   b. Create a custom role in Google Cloud with the permissions defined in the YAML file.
   `gcloud iam roles create dmtoim_convert_tool_role --project=PROJECT_ID \`

`--file=YAML_FILE_PATH`
For more information, refer to Creating and managing custom roles.

c. Attach the custom role to the service account that you'll use to create the VM.

d. Add the `roles/iam.serviceAccountUser` role to this service account. Refer to Service accounts overview.

2. Create a VM with the following configurations. You run the tool on this VM.
   - Machine Type: Google Compute Engine machine type e2-medium
   - OS: Based on your requirement, select either of these images:
     - Ubuntu 25.10 AMD64 Minimal (image: ubuntu-minimal-2510-amd64)
     - SUSE Linux Enterprise Server 15 SP7 x86_64
   - Networking: Firewall allowing HTTP and HTTPs
   - Disk Size: 20GB
   - Security: Service accounts: the service account you created
   - Security: Access Scope - access set for each API:
     - Cloud Platform: Enabled
     - Compute Engine: Read only
     - Storage: Read only (default)
     - Google Cloud Logging (previously Stackdriver Logging) API: Write only (default)
     - Stackdriver Monitoring (now part of Google Cloud Operations) API: Write only (default)
     - Service Management: Read only (default)
     - Service Control: Enabled (default)
     - Google Cloud Trace (previously Stackdriver Trace): Write only (default)
3. Connect to the newly created VM using SSH: `gcloud compute ssh dmtoim-convert-executor-vm --zone <region where VM is deployed>`
4. Download the conversion tool from the NetApp Support site by using your NSS credentials: `wget <download link from NetApp Support site>`
5. Extract the downloaded TAR file: `unzip <downloaded file name>`

Ubuntu

1. Download and install these prerequisite packages:
    - Docker: 28.2.2 build 28.2.2-0ubuntu1 or later
    - Terraform: 1.14.1 or later
    - Python: 3.13.7, python3-pip, python3 venv

    ```
    sudo apt-get update
    sudo apt-get install python3-pip python3-venv -y
    wget -O - https://apt.releases.hashicorp.com/gpg | sudo gpg
    --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg
    echo "deb [arch=$(dpkg --print-architecture) signed-
    by=/usr/share/keyrings/hashicorp-archive-keyring.gpg]
    https://apt.releases.hashicorp.com noble main" | sudo tee
    /etc/apt/sources.list.d/hashicorp.list
    sudo apt update && sudo apt install terraform
    sudo apt-get install -y docker.io
    sudo systemctl start docker
    ```

    Google Cloud CLI `gcloud` is preinstalled on the VM.

SUSE Linux Enterprise Server

1. Set up Python: `sudo update-alternatives --install /usr/bin/python3 python3 /usr/bin/python3.11 2`
2. Install pip3 for installing the package: `python3.11 -m ensurepip --upgrade`
3. Install Terraform:

    ```
    wget
    https://releases.hashicorp.com/terraform/1.7.4/terraform_1.7.4_linux
    _amd64.zip
    unzip terraform_1.7.4_linux_amd64.zip
    sudo mv terraform /usr/local/bin/
    rm terraform_1.7.4_linux_amd64.zip
    ```

4. Install Google Cloud SDK (gcloud)

    ```
    curl https://sdk.cloud.google.com | bash
    exec -l $SHELL
    ```

Run the conversion tool

These steps are for both Ubuntu and SUSE Linux Enterprise Server for running the conversion tool.

Steps

1. Add the current user to the Docker group, so that the tool can use Docker without `sudo` privileges.

   ```
   sudo usermod -aG docker $USER
   newgrp docker
   ```

2. Install the conversion tool:

   ```
   cd <folder where you extracted the tool>
    ./install.sh
   ```

   This installs the tool in an isolated environment, `dmconvert-venv`, and verifies that all required software packages are installed.

3. Enter the environment where the tool is installed: `source dmconvert-venv/bin/activate`

4. Run the conversion tool as a `non-sudo` user. Ensure that you use the same service account as the Console agent's service account, and that the service account has all the necessary permissions for Google Cloud Infrastructure Manager.

   ```
   dmconvert \
   --project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
   deployment> \
   --cvo-name=<Cloud Volumes ONTAP system name> \
   --service-account=<the service account attached to the Console agent>
   ```

   Run the tool in private mode deployments

   Specify the `--worker-pool` parameter to run the tool in private mode deployments. For worker pool configuration, refer to Infrastructure Manager configuration for private mode deployments.

   ```
   dmconvert \
   --project-id=<the Google Cloud project ID for the Cloud Volumes
   ONTAP deployment> \
   --cvo-name=<Cloud Volumes ONTAP system name> \
   --service-account=<the service account attached to the Console
   agent> \
   --worker-pool=<worker pool name>
   ```

After you finish

The tool displays a list of all Cloud Volumes ONTAP systems and SVM details. When it finishes running, you can see the statuses of all the converted systems. Each converted system appears in the Google Console under Infrastructure Manager in a *<system-name-imdeploy>* format, indicating that the Console now uses Infrastructure Manager APIs to manage that Cloud Volumes ONTAP system.

> Post conversion, do not delete the deployment object for Deployment Manager in the Google Cloud Console. This deployment object contains information that you might need to roll back the converted system.

If you need to roll back the conversion, you must use the same VM. If you have converted all systems and do not need to roll back to Deployment Manager, you can delete the VM.

Roll back the conversion

If you don't want to continue with the conversion, you can roll back to Deployment Manager by following these steps:

Steps

1. On the same VM that you created for running the tool, run this command:

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent> \
--rollback
```

2. Wait till the rollback is complete.

Related links

- NetApp Console Agent 4.2.0 Release Notes
- Permissions required for Google Cloud Infrastructure Manager

Administer Cloud Volumes ONTAP using System Manager

Advanced storage management capabilities in Cloud Volumes ONTAP are available through ONTAP System Manager, a management interface provided with ONTAP systems. You can access System Manager directly from the NetApp Console.

Features

You can perform various storage management functions using ONTAP System Manager in the Console. The following list includes some of those functionalities, though this list is not exhaustive:

- Advanced storage management: Manage consistency groups, shares, qtrees, quotas, and Storage VMs.
- Volume move: Move a volume to a different aggregate.
- Networking management: Manage IPspaces, network interfaces, portsets, and ethernet ports.
- Manage FlexGroup volumes: You can create and manage FlexGroup volumes only through System

Manager. The Console does not support FlexGroup volume creation.

- 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.
- ONTAP S3 object storage management: ONTAP S3 storage management capabilities in Cloud Volumes ONTAP are available only in System Manager, and not in the Console.

Supported configurations

- Advanced storage management through ONTAP System Manager is available in 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:

- NetApp Cloud Tiering: Cloud Volumes ONTAP does not support Cloud Tiering. You should set up tiering of data to object storage directly from the 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 the Standard View.
- Firmware upgrades: Cloud Volumes ONTAP does not support automatic firmware updates from the **Cluster > Settings** page of the System Manager.
- Role-based access control: Role-based access control from System Manager is not supported.
- SMB Continuous Availability (CA): Cloud Volumes ONTAP does not support continuously available SMB shares for nondisruptive operations.

Configure authentication for accessing System Manager

As an administrator, you can activate authentication for users accessing ONTAP System Manager from the Console. You can determine the right level of access permissions based on the ONTAP user roles, and enable or disable authentication as needed. If you enable authentication, then users need to enter their ONTAP user credentials every time they access System Manager from the Console or when the page is reloaded, because the Console doesn't store the credentials internally. If you disable authentication, users can access System Manager using the admin credentials.

> ⓘ This setting is applicable for each Console agent for the ONTAP users in your organization or account, irrespective of the Cloud Volumes ONTAP system.

Required permissions

You need to be assigned the organization or account admin privileges to modify the Console agent settings for Cloud Volumes ONTAP user authentication.

Steps

1. From the left navigation pane, go to **Administration > Agents**.
2. Click the ••• icon for the required Console agent and select **Edit Console agent**.
3. Under **Force user credentials**, select the **Enable/Disable** check box. By default, authentication is disabled.

If you set this value to **Enable**, authentication is reset, and you have to modify any existing workflows to accommodate this change.

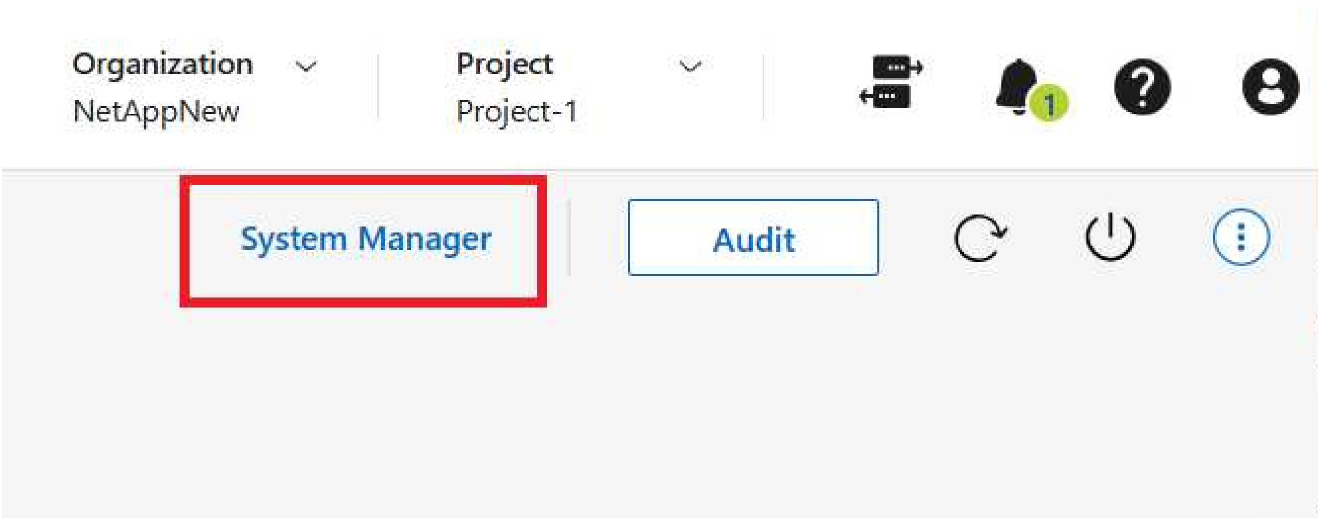
4. Click **Save**.

Get started with System Manager

You can access ONTAP System Manager from a Cloud Volumes ONTAP system.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, double click the required Cloud Volumes ONTAP system.
3. Click **System Manager**.



4. If prompted, enter your ONTAP user credentials and click **Login**.
5. If a confirmation message appears, read through it and click **Close**.

Use System Manager to manage your Cloud Volumes ONTAP system. You can click **Go back** to return to the Console.

Help with using System Manager

If you need help using System Manager with Cloud Volumes ONTAP, you can refer to the ONTAP documentation for step-by-step instructions. Here are a few ONTAP documentation links that might help:

- ONTAP roles, applications, and authentication
- Use System Manager to access a cluster.
- Volume and LUN management
- Network management
- Data protection
- Create continuously available SMB shares

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.

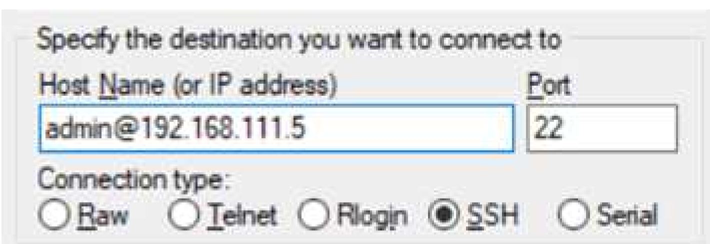
> When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

Steps

1. In the NetApp Console, identify the IP address of the cluster management interface:
   a. From the left navigation menu, select **Storage > Management**.
   b. On the **Systems** page, select the Cloud Volumes ONTAP system.
   c. 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 for Cloud Volumes ONTAP

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 HTTPS traffic to the following endpoints so Cloud Volumes ONTAP can send AutoSupport messages:

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

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

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.

> If you’re using an HA pair, the HA mediator doesn’t require outbound internet access.

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 the ONTAP documentation: Set up AutoSupport.

Troubleshoot your AutoSupport configuration

If an outbound connection isn’t available and the Console can’t configure your Cloud Volumes ONTAP system to use the Console agent as a proxy server, you’ll receive a notification from the Console that your system is unable to send AutoSupport messages. Follow these steps to address this issue.

Steps

1. Connect securely (using SSH) to the Cloud Volumes ONTAP system to use the ONTAP CLI.

   Learn how to SSH to Cloud Volumes ONTAP.

2. Check the detailed status of the AutoSupport subsystem:

   ```
   autosupport check show-details
   ```

   The response looks like this:

```
    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` it means that AutoSupport is configured properly and messages can be sent.

3. If not, 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 Console agent as a proxy:

   ```
   autosupport modify -proxy-url http://<console agent private ip>:3128
   ```

5. Verify the AutoSupport status again:

   ```
   autosupport check show-details
   ```

6. If the status is still failed, validate that there is connectivity between Cloud Volumes ONTAP and the Console agent over port `3128`.
7. If the status is still failed after verification, SSH to the Console agent.

   Learn more about Connecting to the Linux VM for the Console agent

8. Go to `/opt/application/netapp/cloudmanager/docker_occm/data/`.
9. Open the proxy configuration file `squid.conf`. This is the structure of the file:

```
        http_port 3128
        acl netapp_support dst support.netapp.com
        http_access allow netapp_support
        request_header_max_size 21 KB
        reply_header_max_size 21 KB
        http_access deny all
        httpd_suppress_version_string on
```

10. If your file doesn't have an entry for the CIDR block of the Cloud Volumes ONTAP system, add a new entry and allow access:

    `acl cvonet src <cidr>`

    `http_access allow cvonet`

    Here's an example:

```
        http_port 3128
        acl netapp_support dst support.netapp.com
        acl cvonet src <cidr>
        http_access allow netapp_support
        http_access allow cvonet
        request_header_max_size 21 KB
        reply_header_max_size 21 KB
        http_access deny all
        httpd_suppress_version_string on
```

11. After editing the config file, restart the proxy container as `sudo`. Then, depending on whether you're using Docker or Podman, run these commands:

    For Docker, run `docker restart squid`.

    If you are using Podman, run `podman restart squid`.

12. Go back to the ONTAP CLI and verify that Cloud Volumes ONTAP can send AutoSupport messages:

    `autosupport check show-details`

Related links

- Networking requirements for Cloud Volumes ONTAP in AWS
- Networking requirements for Cloud Volumes ONTAP in Azure
- Networking requirements for Cloud Volumes ONTAP in Google Cloud

Configure EMS for Cloud Volumes ONTAP systems

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 the ONTAP documentation: EMS configuration overview.

Concepts

Licensing

Licensing for Cloud Volumes ONTAP

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. For more information about consumption models or purchase options in capacity-based licenses, refer to Learn more about capacity-based licenses.

Keystone Subscription

A pay-as-you-grow subscription-based service that delivers a seamless hybrid cloud experience for High Availability (HA) pairs.

The following sections provide more details about each of these options.

> Support is not available for the use of licensed features without a license.

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.

> While the actual usage and metering for the products and services managed in the NetApp Console are always calculated in GiB and TiB, the terms GB/GiB and TB/TiB are used interchangeably. This is reflected in the Cloud marketplace listings, price quotes, listing descriptions, and in other supporting documentation.

Packages

The following capacity-based packages are available for Cloud Volumes ONTAP. For more information about capacity-based license packages, refer to Learn more about capacity-based licenses.

For a list of supported VM types with the following capacity-based packages, refer to:

* Supported configurations in Azure
* Supported configurations in Google Cloud

Freemium

Provides all Cloud Volumes ONTAP features free of charge from NetApp (cloud provider charges still apply). A Freemium package has these characteristics:

* 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, for any cloud provider.
* If the provisioned capacity for a Cloud Volumes ONTAP system exceeds 500 GiB, the Console converts the system to an Essentials package.

  As soon as a system is converted to the Essentials package, minimum charging applies to it.

  A Cloud Volumes ONTAP system that has been converted into an Essentials package cannot be switched back to Freemium even if the provisioned capacity is reduced to less than 500 GiB. Other systems with less than 500 GiB of provisioned capacity stay on Freemium (as long as they were deployed using the Freemium offering).

Essentials

You can pay by capacity 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 NetApp Backup and Recovery, but only for Cloud Volumes ONTAP systems that use the Professional package.

  > A pay-as-you-go (PAYGO) subscription is required for Backup and Recovery, however no charges will be incurred for using this service. For more information on setting up licensing for Backup and Recovery, refer to Set up licensing for Backup and Recovery.

* Add on any of NetApp's cloud data services at extra cost

Availability of capacity-based licenses

The availability of the PAYGO and BYOL licenses for Cloud Volumes ONTAP systems requires the Console agent to be up and running.

Learn about Console agents.

> NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAPP.

How to get started

Learn how to get started with capacity-based licensing:

- Set up licensing for Cloud Volumes ONTAP in AWS
- Set up licensing for Cloud Volumes ONTAP in Azure
- Set up licensing for Cloud Volumes ONTAP in Google Cloud

Keystone 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 Subscription.

The provisioned capacity for each volume is aggregated and compared to the committed capacity on your Keystone Subscription periodically, and any overages are charged as burst on your Keystone Subscription.

Learn more about NetApp Keystone.

Supported configurations

Keystone Subscriptions are supported with HA pairs. This licensing option isn't supported with single-node systems at this time.

Capacity limit

In the capacity-based licensing model, each Cloud Volumes ONTAP system supports tiering to object storage, and the total tiered capacity can scale up to the cloud provider's bucket limit. Although the license does not impose capacity restrictions, follow the FabricPool Best Practices to ensure optimal performance, reliability, and cost efficiency when configuring and managing tiering.

For information about the capacity limits of each cloud provider, refer to their documentation:

- AWS documentation
- Azure documentation for managed disks and Azure documentation for blob storage
- Google Cloud documentation

How to get started

Learn how to get started with a Keystone Subscription:

* Set up licensing for Cloud Volumes ONTAP in AWS
* Set up licensing for Cloud Volumes ONTAP in Azure
* Set up licensing for Cloud Volumes ONTAP in Google Cloud

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. By-node charging has been replaced with the by-capacity charging methods described above.

NetApp has planned the end of availability (EOA) and support (EOS) of node-based licensing. After the EOA and EOS, node-based licenses will need to be converted to capacity-based licenses.

For information, refer to Customer communique: CPC-00589.

End of availability of node-based licenses

Beginning on 11 November, 2024, the limited availability of node-based licenses has been terminated. The support for node-based licensing ends on 31 December, 2024.

If you have a valid node-based contract that extends beyond the EOA date, you can continue to use the license until the contract expires. Once the contract expires, it will be necessary to transition to the capacity-based licensing model. If you don't have a long-term contract for a Cloud Volumes ONTAP node, it is important to plan your conversion before the EOS date.

Learn more about each license type and the impact of EOA on it from this table:

License type	Impact after EOA
Valid node-based license purchased through bring your own license (BYOL)	License remains valid till expiration. Existing unused node-based licenses can be used for deploying new Cloud Volumes ONTAP systems.
Expired node-based license purchased through BYOL	You won't be entitled to deploy new Cloud Volumes ONTAP systems using this license. The existing systems might continue to work, but you won't receive any support or updates for your systems post the EOS date.
Valid node-based license with PAYGO subscription	Will cease to receive NetApp support post the EOS date, until you transition to a capacity-based license.

Exclusions

NetApp recognizes that certain situations require special consideration, and EOA and EOS of node-based licensing will not apply to the following cases:

* U.S. Public Sector customers
* Deployments in private mode
* China region deployments of Cloud Volumes ONTAP in AWS

For these particular scenarios, NetApp will offer support to address the unique licensing requirements in compliance with contractual obligations and operational needs.

> Even in these scenarios, new node-based licenses and license renewals are valid for a maximum of one year from the date of approval.

License conversion

The Console enables a seamless conversion of node-based licenses to capacity based through the license conversion tool. For information about EOA of node-based licensing, refer to End of availability of node-based licenses.

Before transitioning, it is good to familiarize yourself with the difference between the two licensing models. Node-based licensing includes fixed capacity for each ONTAP instance, which can restrict flexibility. Capacity-based licensing, on the other hand, allows for a shared pool of storage across multiple instances, offering enhanced flexibility, optimizing resource utilization, and reducing the potential for financial penalties when redistributing workloads. Capacity-based charging seamlessly adjusts to changing storage requirements.

To know how you can perform this conversion, refer to Convert a Cloud Volumes ONTAP node-based license to capacity-based license.

> Conversion of a system from capacity-based to node-based licensing is not supported.

Learn more about capacity-based licenses for Cloud Volumes ONTAP

You should be familiar with the charging and capacity usage for capacity-based licenses.

Consumption models or license purchase options

Capacity-based licensing packages are available with the following consumption models or purchase options:

- **BYOL**: Bring your own license (BYOL). A license purchased from NetApp that can be used to deploy Cloud Volumes ONTAP in any cloud provider.

  > NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP.

- **PAYGO**: A pay-as-you-go (PAYGO) subscription is 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. NetApp has restricted BYOL licensing. When your BYOL licenses expire, you are required to replace them with cloud marketplace subscriptions.

  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.
- Only single-node systems with BYOL are supported in China regions. China region deployments are exempt from BYOL licensing restrictions.

Changing of license 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.

For information about converting node-based licenses to capacity-based, see

How you are charged for supported storage types and packages

Charging in Cloud Volumes ONTAP is based on a number of factors, such as packages and volume types. Capacity-based licensing packages are available with Cloud Volumes ONTAP 9.7 and later.

For details about pricing, go to the NetApp Console website.

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.

Read/write volumes

If you create or use a writable (read/write) volume, it is considered a primary volume and is charged for the provisioned capacity based on the minimum charge per storage VM (SVM). Examples include FlexVol read/write volumes, SnapLock audit volumes, and CIFS/NFS audit volumes. All user-created data volumes are charged per your subscription and package type. ONTAP internal volumes that are automatically created and cannot store data, such as SVM root volumes, are not charged.

Essentials packages

With the Essentials package, you're billed by the deployment type (HA or single node) and the volume type (primary or secondary). Pricing from high to low is in the following order: *Essentials Primary HA*, *Essentials Primary Single Node*, *Essentials Secondary HA*, and *Essentials Secondary Single Node*. Alternately, when you purchase a marketplace contract or accept a private offer, capacity charges are the same for any deployment or volume type.

Licensing is based entirely on the volume type created within Cloud Volumes ONTAP systems:

- Essentials Single Node: Read/write volumes created on a Cloud Volumes ONTAP system using one ONTAP node only.
- Essentials HA: Read/write volumes using two ONTAP nodes that can fail over to each other for non-disruptive data access.
- Essentials Secondary Single Node: Data Protection (DP) type volumes (typically SnapMirror or SnapVault destination volumes that are read-only) created on a Cloud Volumes ONTAP system using one ONTAP node only.

  > If a read-only/DP volume becomes a primary volume, the Console considers it as primary data and the charging costs are calculated based on the time the volume was in read/write mode. When the volume is again made read-only/DP, it considers the volume as secondary data again and charges accordingly using the best matching license in the Console.

- Essentials Secondary HA: Data Protection (DP) type volumes (typically SnapMirror or SnapVault destination volumes that are read-only) created on a Cloud Volumes ONTAP system using two ONTAP nodes that can fail over to each other for non-disruptive data access.

Capacity limit

In the capacity-based licensing model, each Cloud Volumes ONTAP system supports tiering to object storage, and the total tiered capacity can scale up to the cloud provider's bucket limit. Although the license does not impose capacity restrictions, follow the FabricPool Best Practices to ensure optimal performance, reliability, and cost efficiency when configuring and managing tiering.

For information about the capacity limits of each cloud provider, refer to their documentation:

- AWS documentation
- Azure documentation for managed disks and Azure documentation for blob storage
- Google Cloud documentation

Max number of systems

With capacity-based licensing, the maximum number of Cloud Volumes ONTAP systems is limited to 24 per NetApp Console organization. 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 systems:

- 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 system 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 system 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 system 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 organization.

If you have a large deployment that requires more then 24 systems, contact your accounts representative or sales team.

Learn about storage limits for AWS, Azure, and Google Cloud.

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 the Console 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.

For the Essentials package, 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. With the Professional package type, the minimum capacity charging of 4 TiB applies regardless of the volume type.

Billing preferences and overages

You can choose how you want to be charged in the **Licenses and subscriptions** section in the Console. Overages occur when your usage exceeds the capacity specified in your license package or annual subscription.

- **NetApp licenses first**: In this model, your usage is first charged against the capacity of your license package (BYOL). If you exceed your license capacity, overages are charged based on your annual marketplace subscription or marketplace on-demand hourly rates (PAYGO). If your BYOL license expires, you must transition to a capacity-based licensing model through the cloud marketplaces. For information, refer to Convert a Cloud Volumes ONTAP node-based license to a capacity-based license.
- **Marketplace subscriptions only**: In this model, your usage is first charged against your annual marketplace subscription. Any additional usage is charged at marketplace on-demand hourly rates (PAYGO). Any unused license capacity is disregarded for billing.

For more information about billing preferences, refer to Learn about billing preferences for licenses and subscriptions.

How overages are charged for Essentials licenses

If you purchase an Essentials license from NetApp (BYOL) and you exceed the licensed capacity for a specific Essentials package, the Console charges overages against a higher-priced Essentials license (if you have one with available capacity). The Console first uses the available capacity that you've paid for before charging against the marketplace. If there is no available capacity with your BYOL license, the exceeded capacity is charged at marketplace on-demand hourly rates (PAYGO) and added to your monthly bill.

Similarly, if you have an annual marketplace contract or a private offer with multiple Essentials packages, and your usage exceeds the committed capacity for a deployment and volume type of a specific package, the Console charges overages against a higher-priced Essentials package based on its available capacity. After that capacity is exhausted, the remaining overage is billed at marketplace on-demand (PAYGO) hourly rates and added to your monthly bill.

For information about Essentials licenses charging, refer to Essentials packages.

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 Console charges the 50 TiB overage against the *Essentials Single Node* license. That license is priced higher than *Essentials Secondary HA*, but it's making use of a license you have already purchased, and it will not add costs to your monthly bill.

In **Administration > Licenses and subscriptions**, you can see 50 TiB charged against the *Essentials Single Node* license.

Here's another 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 100 TiB is provisioned on an HA pair with primary volumes. The license you purchased doesn't have *Essentials Primary HA* committed capacity. The *Essentials Primary HA* license is priced higher than both the *Essentials Primary Single Node* and *Essentials Secondary HA* licenses.

In this example, the Console charges overages at the marketplace rate for the additional 100 TiB. The overage charges will appear on your monthly bill.

Storage

Supported client protocols for Cloud Volumes ONTAP

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

iSCSI

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

NFS

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

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

SMB

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

S3

Cloud Volumes ONTAP supports S3 as an option for scale-out storage. S3 protocol support enables you to configure S3 client access to objects contained in a bucket in a storage VM (SVM).

ONTAP documentation: Learn how S3 multiprotocol works.
ONTAP documentation: Learn how to configure and manage S3 object storage services in ONTAP.

NVMe-TCP

Beginning with ONTAP version 9.12.1, NVMe-TCP is supported for all cloud providers. Cloud Volumes ONTAP supports NVMe-TCP as a block protocol for storage VMs (SVMs) during deployment, and installs the required NVMe licenses automatically.

NetApp Console does not provide any management capabilities for NVMe-TCP.

For more information on configuring NVMe through ONTAP, refer to the ONTAP documentation: Configure a storage VM for NVMe.

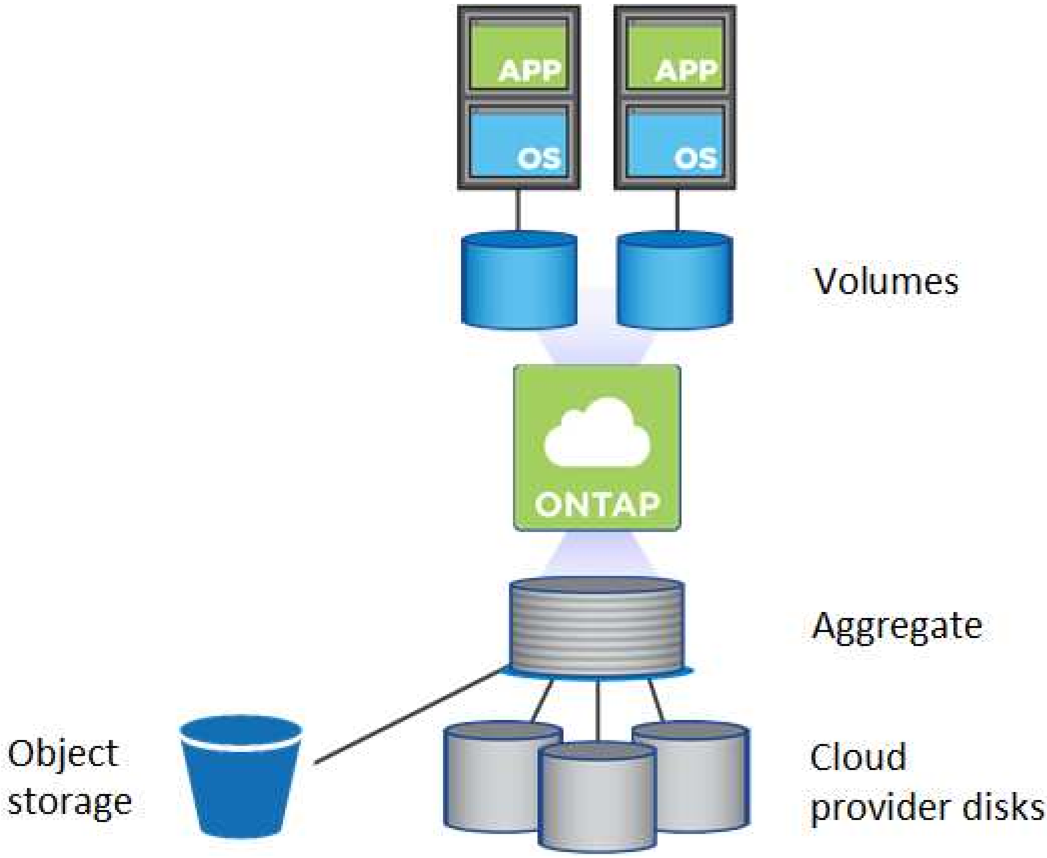
Disks and aggregates used for Cloud Volumes ONTAP clusters

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

> You must create and delete all disks and aggregates from the NetApp Console. 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 the Console creates a 500 GiB aggregate, the usable capacity is 442.94 GiB.

AWS storage

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

EBS storage

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

The maximum disk size is 16 TiB.

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

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

Local NVMe storage

Some EC2 instance types include local NVMe storage, which Cloud Volumes ONTAP uses as Flash Cache.

Related links

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

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 these types of Azure Managed Disks:

- *Premium SSD Managed Disks* provide high performance for I/O-intensive workloads at a higher cost.
- *Premium SSD v2 Managed Disks* provide higher performance with lower latency at a lower cost for both single node and HA pairs, compared to Premium SSD Managed Disks.
- *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 low-cost object storage.

HA pairs

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

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

Related links

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

Google Cloud storage

In Google Cloud, an aggregate can contain up to 6 disks that are all the same size. The maximum disk size is 64 TiB.

The disk type can be either *Zonal SSD persistent disks*, *Zonal Balanced persistent disks*, or *Zonal standard persistent disks*. You can pair persistent disks with a Google Storage bucket to low-cost object storage.

Related links

- Google Cloud documentation: Storage Options
- Review storage limits for Cloud Volumes ONTAP in Google Cloud

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.

Learn about support for AWS Elastic Volumes with Cloud Volumes ONTAP

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

Benefits

- Dynamic disk growth

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

- Better performance

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

- Larger aggregates

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

  Note that total system capacity limits remain the same.

AWS Documentation: Learn more about Elastic Volumes from AWS

Supported configurations

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

Cloud Volumes ONTAP version

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

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

EBS disk types

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

Required AWS permissions

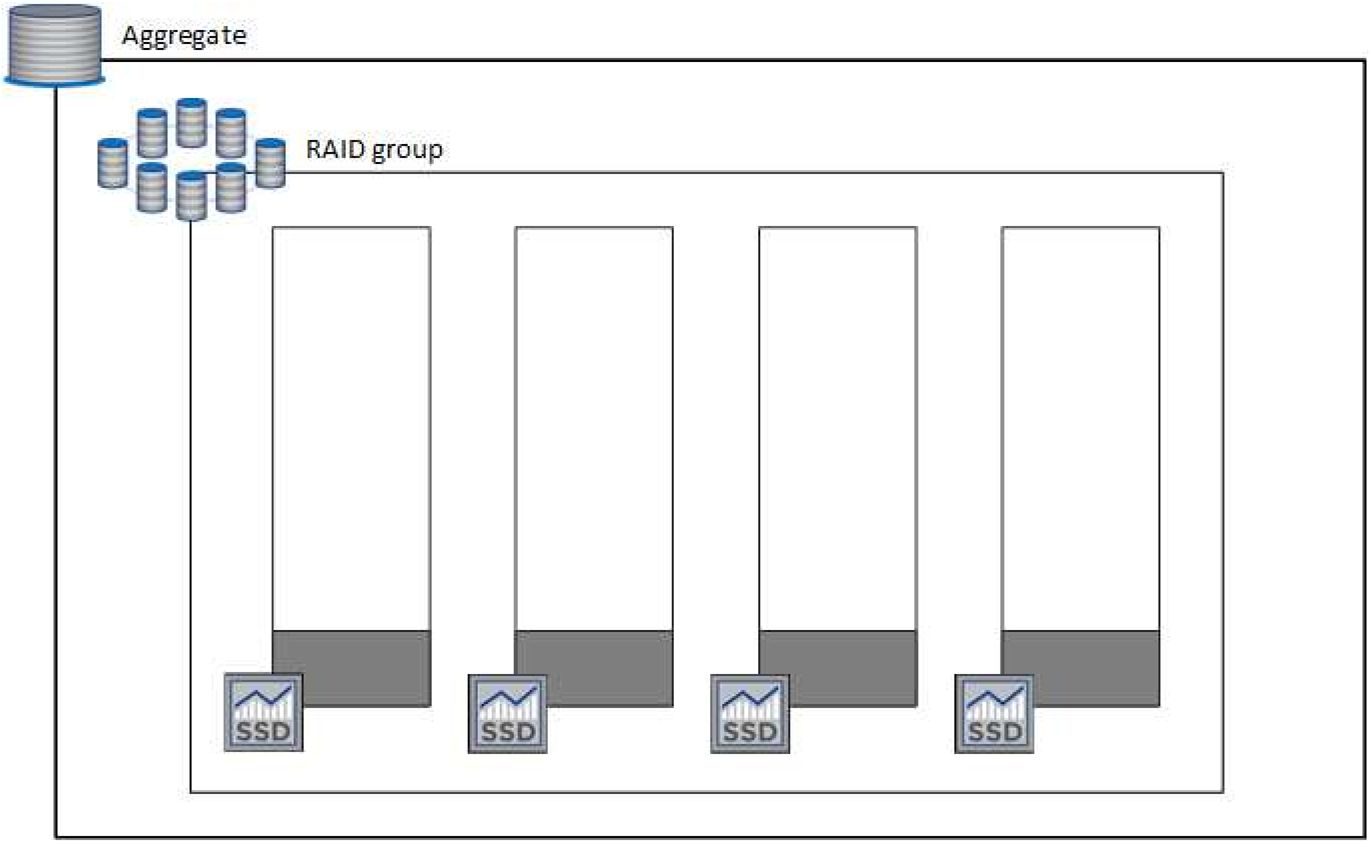
Starting with the 3.9.19 release, the Console agent requires the following permissions to enable and manage the Elastic Volumes feature on a Cloud Volumes ONTAP aggregate:

- ec2:DescribeVolumesModifications
- ec2:ModifyVolume

These permissions are included in the policies provided by NetApp

How support for Elastic Volumes works

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



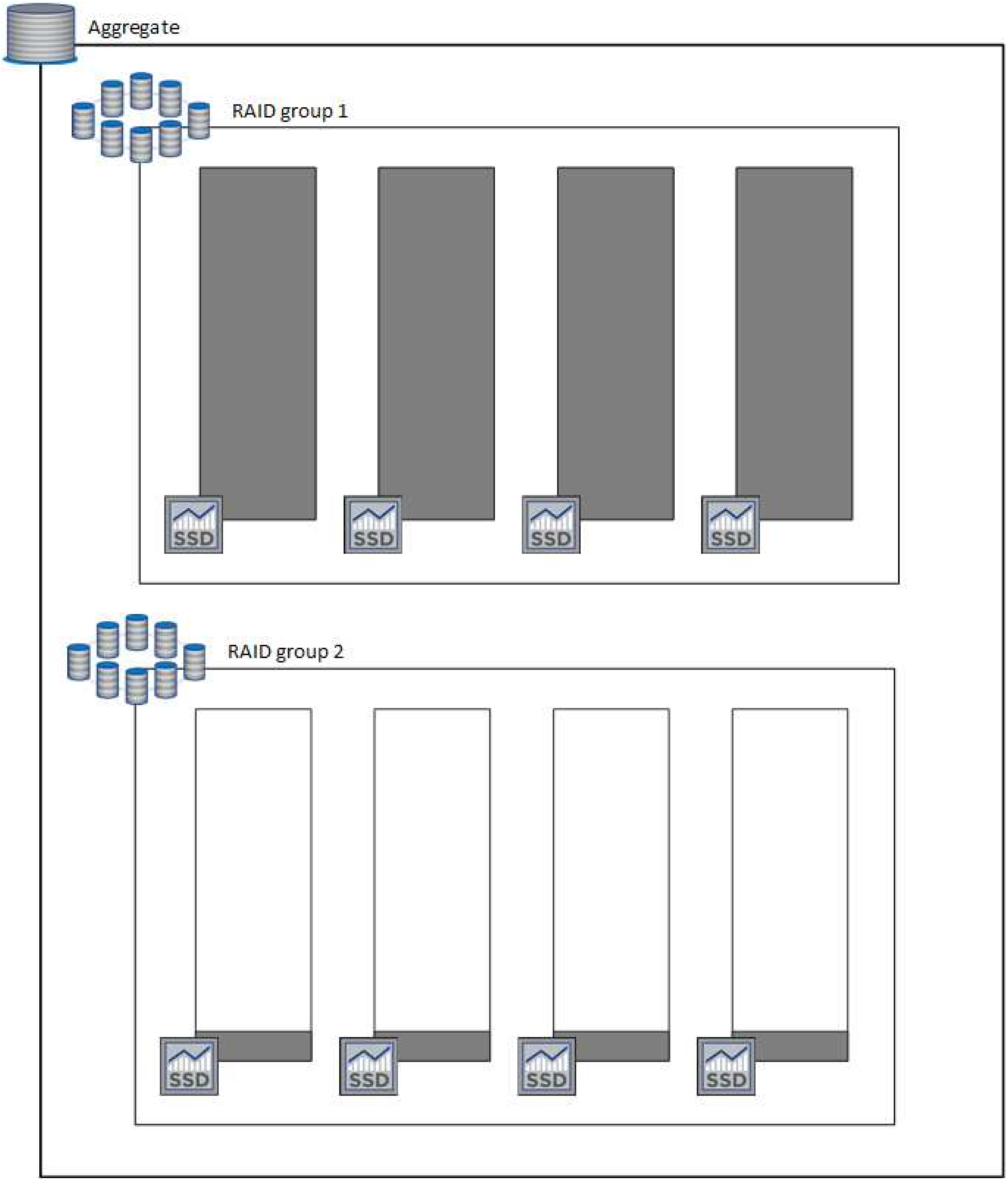
When the Console creates an aggregate, it starts with one RAID group. If additional capacity is needed, it grows the aggregate by increasing the capacity of all disks in the RAID group by the same amount. The capacity increase is either a minimum of 256 GiB or 10% of the aggregate's size.

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

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

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

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



What happens when you create a volume

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

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

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

> While this scenario is unlikely, it's possible in two cases:
>
> - You explicitly disabled the Elastic Volumes feature when creating an aggregate from the API.
> - You created a new Cloud Volumes ONTAP system from the user interface, in which case the Elastic Volumes feature is disabled on the initial aggregate. Review Limitations below to learn more.

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

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

Capacity Management Mode

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

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

Learn more about the Capacity Management Mode.

Limitations

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

How to work with Elastic Volumes

You can perform these tasks with Elastic Volumes:

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

  Learn how to create Cloud Volumes ONTAP system

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

  If you create a volume that uses gp3 or io1 disks, the Console automatically creates the volume on an aggregate that has Elastic Volumes enabled. For more details, refer to What happens when you create a volume.

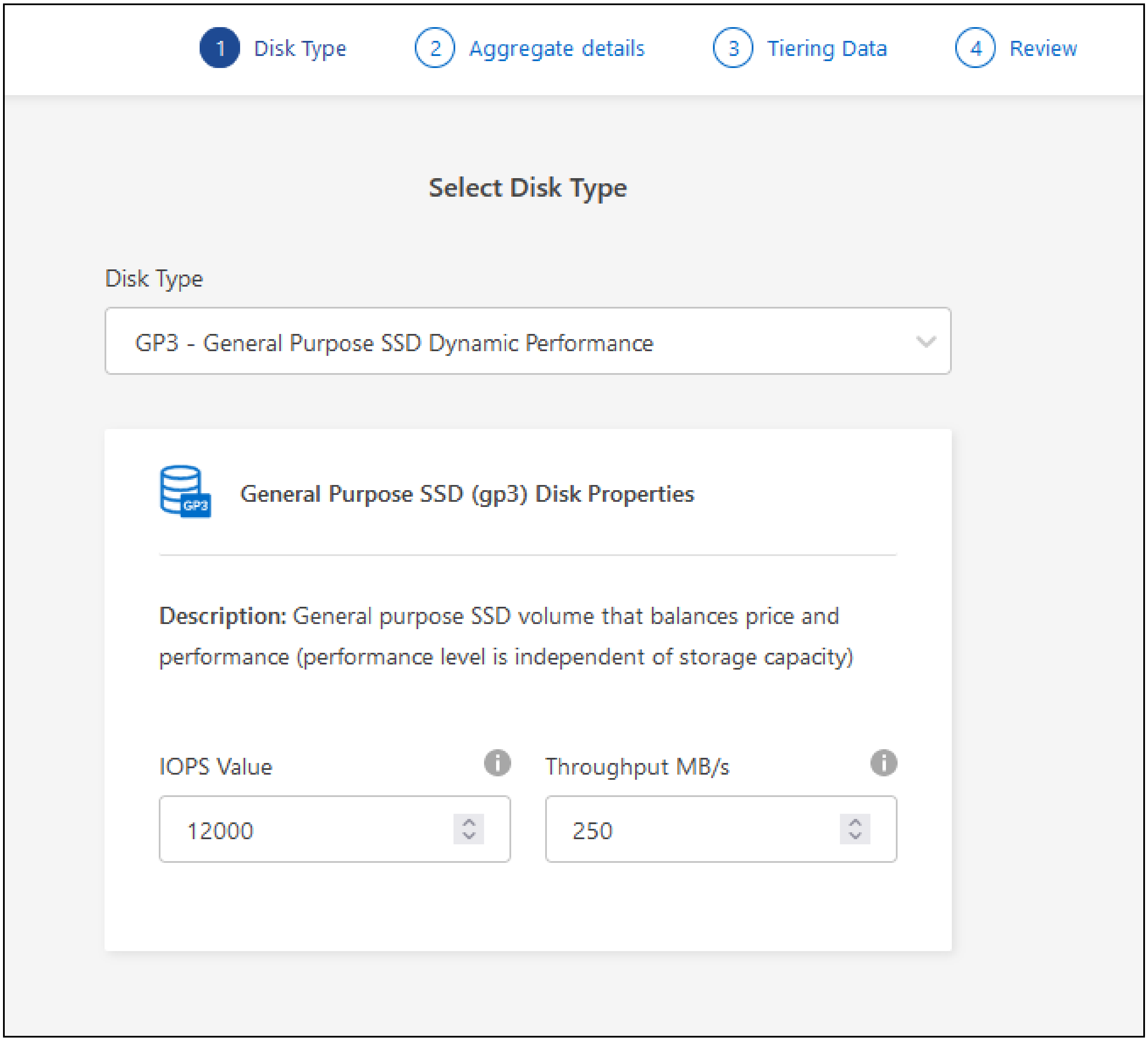
  Learn how to create volumes.

- Create a new aggregate that has Elastic Volumes enabled

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

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

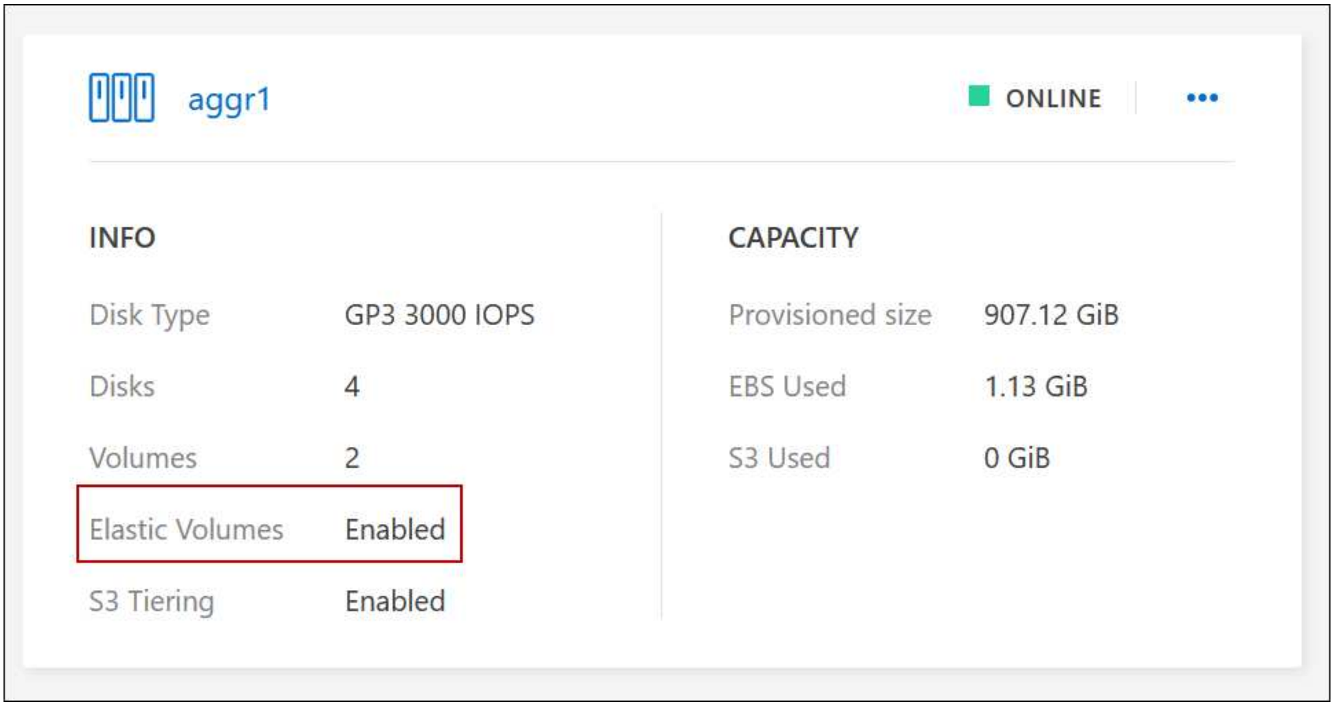
The following screenshot shows an example of a new aggregate comprised of gp3 disks.



Learn how to create aggregates.

- Identify aggregates that have Elastic Volumes enabled

  When you go to the Advanced Allocation page, you can identify whether the Elastic Volumes feature is enabled on an aggregate. In the following example, aggr1 has Elastic Volumes enabled.



- Add capacity to an aggregate

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

  Learn how to increase aggregate capacity.

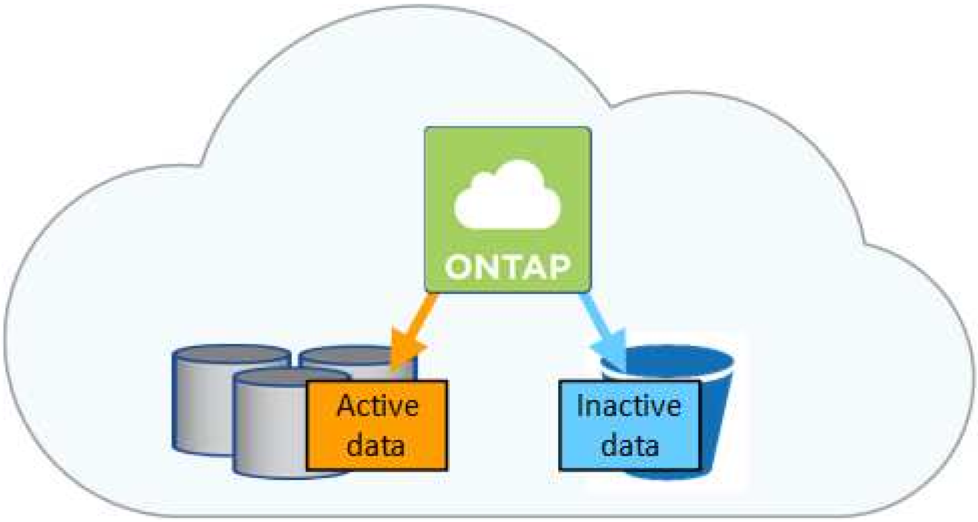
- Replicate data to an aggregate that has Elastic Volumes enabled

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

  Learn how to set up data replication

Learn about data tiering with Cloud Volumes ONTAP in AWS, Azure, or Google Cloud

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. Cloud Volumes ONTAP provides data tiering for all Cloud Volumes ONTAP clusters without an additional license. When you enable data tiering, data tiered to object storage incurs charges. Refer to your cloud provider's documentation for details about object storage costs.

Data tiering in AWS

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

Performance tier

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

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

Capacity tier

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

The NetApp Console creates a single S3 bucket for each system and names it fabric-pool-*cluster unique identifier*. A different S3 bucket is not created for each volume.

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

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

Storage classes

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

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

Access costs are higher if you access the data, so consider this before changing the storage class. Amazon S3 documentation: Learn more about Amazon S3 storage classes.

You can select a storage class when you create the system and you can change it any time afterwards. For instructions on changing the storage class, refer to Tier inactive data to low-cost object storage.

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

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.

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

The Console creates the storage account with the following settings:

- Access tier: Hot
- Performance: Standard
- Redundancy: Accordingly to Cloud Volume ONTAP Deployment
  - Single availability zone: Locally-redundant storage (LRS)
  - Multiple availability zone: Zone-redundant storage (ZRS)
- 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 in the capacity tier.

If you don't plan to access the inactive data in the capacity tier, you can choose the *cool* storage tier, where the inactive data is retained for a minimum of 30 days. You can also opt for the *cold* tier, where the inactive data is stored for a minimum of 90 days. Based on your storage requirements and cost considerations, you can select the tier that best suits your needs. When you change the storage tier to *cool* or *cold*, the inactive capacity tier data moves directly to the cool or cold storage tier. The cool and cold tiers offer lower storage costs compared to the hot tier, but they come with higher access costs, so take that into consideration before you change the storage tier. Refer to Microsoft Azure documentation: Learn more about Azure Blob storage access tiers.

You can select a storage tier when you add a Cloud Volumes ONTAP system and you can change it any time afterwards. For details about changing the storage tier, refer to Tier inactive data to low-cost object storage.

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

Data tiering in Google Cloud

When you enable data tiering in Google Cloud, Cloud Volumes ONTAP uses persistent disks as a performance tier for hot data and a Google Cloud Storage bucket as a capacity tier for inactive data.

Performance tier

The performance tier can be either SSD persistent disks, balanced persistent disks, or standard persistent disks.

Capacity tier

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

The Console creates a bucket for each system and names it fabric-pool-*cluster unique identifier*. A different bucket is not created for each volume.

When the Console creates the bucket, it uses the following default settings:

- Location type: Region
- Storage class: Standard
- Public access: Subject to object ACLs
- Access control: Fine-grained
- Protection: None
- Data encryption: Google-managed key

Storage classes

The default storage class for tiered data is the *Standard Storage* class. If the data is infrequently accessed, you can reduce your storage costs by changing to *Nearline Storage* or *Coldline Storage*. When you change the storage class, subsequent inactive data moves directly to the class that you selected.

> Any existing inactive data will maintain the default storage class when you change the storage class. To change the storage class for existing inactive data, you must perform the designation manually.

The access costs are higher if you do access the data, so take that into consideration before you change the storage class. To learn more, refer to the Google Cloud documentation: Storage classes.

You can select a storage tier when you create the system and you can change it any time afterwards. For details about changing the storage class, refer to Tier inactive data to low-cost object storage.

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

Data tiering and capacity limits

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

Volume tiering policies

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

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

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

The Console 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.

Replication

When you replicate a volume, you can choose whether to tier the data to object storage. If you do, the Console applies the **Backup** policy to the data protection volume. Starting with Cloud Volumes ONTAP 9.6, the **All** tiering policy replaces the backup policy. When a replication relationship is deleted, the destination volume retains the tiering policy that was in effect during replication.

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, refer to Tier inactive data to low-cost object storage.

Cloud Volumes ONTAP storage management

The NetApp Console provides simplified and advanced management of Cloud Volumes ONTAP storage.

> You must create and delete all disks and aggregates directly from the Console. 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

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

Simplified provisioning

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

When you create a volume, the Console does one of three things:

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

  In the case of an aggregate in AWS that supports Elastic Volumes, it also increases the size of the disks in a RAID group. Learn more about support for Elastic Volumes.

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

The Console 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.

Disk size selection for aggregates in AWS

When the Console creates new aggregates for Cloud Volumes ONTAP in AWS, it gradually increases disk sizes as aggregate numbers increase to maximize system capacity before reaching AWS data disk limits.

For example, the Console might choose the following disk sizes:

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

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

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

Advanced allocation

You can also manage aggregates. 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 organization or account admin can configure the Console to notify you of storage capacity decisions or whether to automatically manage capacity requirements for you.

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

Automatic capacity management

The Capacity Management Mode is set to automatic by default. In this mode, the Console checks the free space ratio every 15 minutes to determine if the free space ratio falls below the specified threshold. If more capacity is needed, it initiates purchase of new disks, deletes unused collections of disks (aggregates), moves volumes between aggregates as required, and attempts to prevent disk failure.

The following examples illustrate how this mode works:

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

  In the case of an aggregate in AWS that supports Elastic Volumes, it also increases the size of the disks in a RAID group. Learn more about support for Elastic Volumes.

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

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

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

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

Management of LUNs with automatic capacity management

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

Manual capacity management

If the organization or account admin sets the **Capacity Management Mode** to manual, the Console informs you to take appropriate actions for capacity decisions. 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

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

Normal write speed

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

Normal write speed is the default option.

High write speed

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

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

When to use high write speed

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

Recommendations when using high write speed

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

High write speed with an HA pair in AWS

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

Learn more about HA pairs in AWS.

Configurations that support high write speed

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

AWS

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

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

Learn more about the Amazon EC2 instances that Cloud Volumes ONTAP supports.

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.

Google Cloud

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

If you use an HA pair, Cloud Volumes ONTAP supports high write speed with several VM types, starting with the 9.13.0 release. Go to the Cloud Volumes ONTAP Release Notes to view the VM types that support high write speed.

Learn more about the Google Cloud machine types that Cloud Volumes ONTAP supports.

How to select a write speed

You can choose a write speed when you add a new Cloud Volumes ONTAP system and you can change the write speed for an existing system.

What to expect if data loss occurs

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

* Cloud Volumes ONTAP 9.12.1 or later

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

* Cloud Volumes ONTAP 9.11.0 to 9.11.1

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

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

* Cloud Volumes ONTAP 9.8 to 9.10.1

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

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

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

How to stop data access if data loss occurs

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

To enable the NVFAIL option

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

To check NVFAIL settings

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

To disable the NVFAIL option

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

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

To check the NVFAIL state

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

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

To clear the NVFAIL state

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

Flash Cache

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

What's Flash Cache?

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

Supported configurations

Flash Cache is supported with specific Cloud Volumes ONTAP configurations. View supported configurations in the Cloud Volumes ONTAP Release Notes

Limitations

- When configuring Flash Cache for Cloud Volumes ONTAP 9.12.0 or earlier in AWS, compression must be disabled on all volumes to take advantage of the Flash Cache performance improvements. When you deploy or upgrade to Cloud Volumes ONTAP 9.12.1 or later, you don't need to disable compression.

  Skip selecting storage efficiency settings when creating a volume from the NetApp Console, 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.

Related topics

- Supported configurations for Cloud Volumes ONTAP in AWS
- Supported configurations for Cloud Volumes ONTAP in Azure
- Supported configurations for Cloud Volumes ONTAP in Google Cloud

Learn about WORM storage on Cloud Volumes ONTAP

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.

The WORM feature is available for use with bring your own license (BYOL) and marketplace subscriptions for your licenses at no additional cost. Contact your NetApp sales representative to add WORM to your current license.

How WORM storage works

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

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

Activating WORM storage

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

Version 9.10.1 and later

Beginning with Cloud Volumes ONTAP 9.10.1, you have the option to enable or disable WORM at the volume level.

When you add a Cloud Volumes ONTAP system, you’re prompted to enable or disable WORM storage:

- If you enable WORM storage when adding a system, every volume that you create from the NetApp Console has WORM enabled. But you can use ONTAP System Manager or the ONTAP CLI to create volumes that have WORM disabled.
- If you disable WORM storage when adding a system, every volume that you create from the Console, ONTAP System Manager, or the ONTAP CLI has WORM disabled.

Version 9.10.0 and earlier

You can activate WORM storage on a Cloud Volumes ONTAP system when you add a new system. Every volume that you create from the Console has WORM enabled. You can’t disable WORM storage on individual volumes.

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 the ONTAP documentation on SnapLock.

Enabling WORM on a Cloud Volumes ONTAP system

You can enable WORM storage when creating a Cloud Volumes ONTAP system on the Console. You can also enable WORM on a system if WORM is not enabled on it during creation. After you enable it, you cannot disable WORM.

About this task

- WORM is supported on ONTAP 9.10.1 and later.
- WORM with backup is supported on ONTAP 9.11.1 and later.

Steps

1. On the **Systems** page, double-click the name of the system on which you want to enable WORM.

2. On the Overview tab, click the Features panel and then click the pencil icon next to **WORM**.

   If WORM is already enabled on the system, the pencil icon is disabled.

3. On the **WORM** page, set the retention period for the cluster Compliance Clock.

   For more information, refer to the ONTAP documentation: Initialize the Compliance Clock.

4. Click **Set**.

After you finish

You can verify the status of **WORM** on the Features panel.
After WORM is enabled, the SnapLock license is automatically installed on the cluster. You can view the SnapLock license on ONTAP System Manager.

Deleting WORM files

You can delete WORM files during the retention period using the privileged delete feature.

For instructions, refer to the ONTAP documentation.

WORM and data tiering

When you create a new Cloud Volumes ONTAP 9.8 system or later, you can enable both data tiering and WORM storage together. Enabling data tiering with WORM storage allows you to tier the data to an object store in the cloud.

You should understand the following about enabling both data tiering and WORM storage:

- Data that is tiered to object storage doesn't include the ONTAP WORM functionality. To ensure end-to-end WORM capability, you'll need to set up the bucket permissions correctly.
- The data that is tiered to object storage doesn't carry the WORM functionality, which means technically anyone with full access to buckets and containers can go and delete the objects tiered by ONTAP.
- Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

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 expiration date by removing or editing cloud storage directly from the cloud provider.

Related link

- Create tamperproof Snapshot copies for WORM storage
- Licensing and charging in Cloud Volumes ONTAP

High-availability pairs

Learn about Cloud Volumes ONTAP HA pairs in AWS

A Cloud Volumes ONTAP high-availability (HA) configuration provides nondisruptive operations and fault tolerance. In AWS, data is synchronously mirrored between the two nodes.

HA components

In AWS, Cloud Volumes ONTAP HA configurations include the following components:

- Two Cloud Volumes ONTAP nodes whose data is synchronously mirrored between each other.
- A mediator instance that provides a communication channel between the nodes to assist in storage takeover and giveback processes.

Mediator

Here are some key details about the mediator instance in AWS:

Instance type
t3-micro

Disks
Two st1 disks of 8 GiB and 4 GiB

Operating system
Debian 11

> For Cloud Volumes ONTAP 9.10.0 and earlier, Debian 10 was installed on the mediator.

Upgrades
When you upgrade Cloud Volumes ONTAP, the NetApp Console also updates the mediator instance as needed.

Access to the instance
When you create a Cloud Volumes ONTAP HA pair from the Console, you're prompted to provide a key pair for the mediator instance. You can use that key pair for SSH access using the `admin` user.

Third-party agents
Third-party agents or VM extensions are not supported on the mediator instance.

Storage takeover and giveback

If a node goes down, the other node can serve data for its partner to provide continued data service. Clients can access the same data from the partner node because the data was synchronously mirrored to the partner.

After the node reboots, the partner must resync data before it can return the storage. The time that it takes to resync data depends on how much data was changed while the node was down.

Storage takeover, resync, and giveback are all automatic by default. No user action is required.

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 120 seconds.
  In the event of an outage, data should be available in 120 seconds or less.

HA deployment models

You can ensure the high availability of your data by deploying an HA configuration across multiple availability zones (AZs) or in a single availability zone (AZ). You should review more details about each configuration to choose which best fits your needs.

Multiple availability zones

Deploying an HA configuration in multiple availability zones (AZs) ensures high availability of your data if a failure occurs with an AZ or an instance that runs a Cloud Volumes ONTAP node. You should understand how NAS IP addresses impact data access and storage failover.

NFS and CIFS data access

When an HA configuration is spread across multiple Availability Zones, *floating IP addresses* enable NAS client access. The floating IP addresses, which must be outside of the CIDR blocks for all VPCs in the region, can migrate between nodes when failures occur. They aren't natively accessible to clients that are outside of the VPC, unless you set up an AWS transit gateway.

If you can't set up a transit gateway, private IP addresses are available for NAS clients that are outside the VPC. However, these IP addresses are static—they can't failover between nodes.

You should review requirements for floating IP addresses and route tables before you deploy an HA configuration across multiple availability zones. You must specify the floating IP addresses when you deploy the configuration. The private IP addresses are automatically created.

For more information, refer to AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs.

iSCSI data access

Cross-VPC data communication is not an issue since iSCSI does not use floating IP addresses.

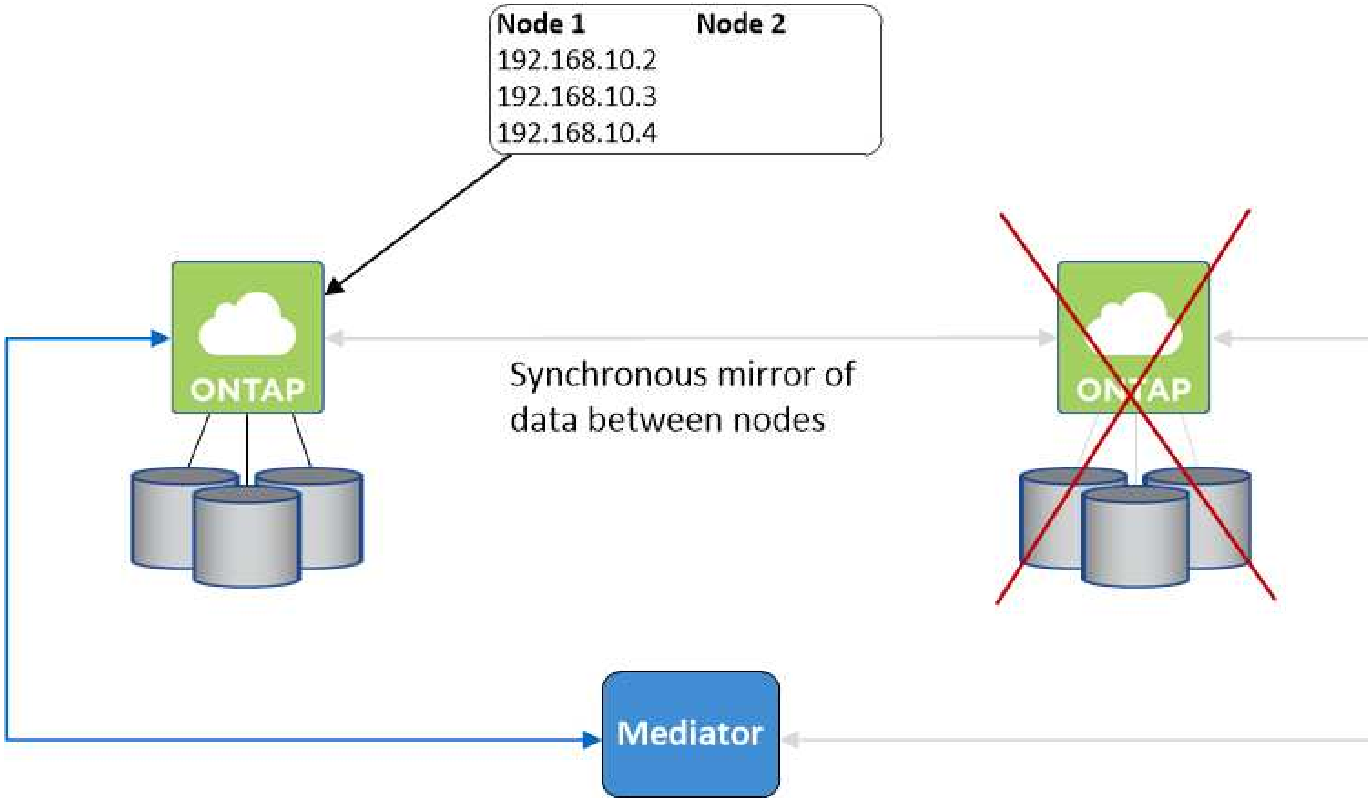
Takeover and giveback for iSCSI

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, refer to the NetApp Interoperability Matrix Tool and the SAN hosts and cloud clients guide for your host operating system.

Takeover and giveback for NAS

When takeover occurs in a NAS configuration using floating IPs, the node's floating IP address that clients use to access data moves to the other node. The following image depicts storage takeover in a NAS configuration using floating IPs. If node 2 goes down, the floating IP address for node 2 moves to node 1.



NAS data IPs used for external VPC access cannot migrate between nodes if failures occur. If a node goes offline, you must manually remount volumes to clients outside the VPC by using the IP address on the other node.

After the failed node comes back online, remount clients to volumes using the original IP address. This step is needed to avoid transferring unnecessary data between two HA nodes, which can cause significant performance and stability impact.

You can locate the correct IP address from the Console by selecting the volume and clicking **Mount Command**.

Single availability zone

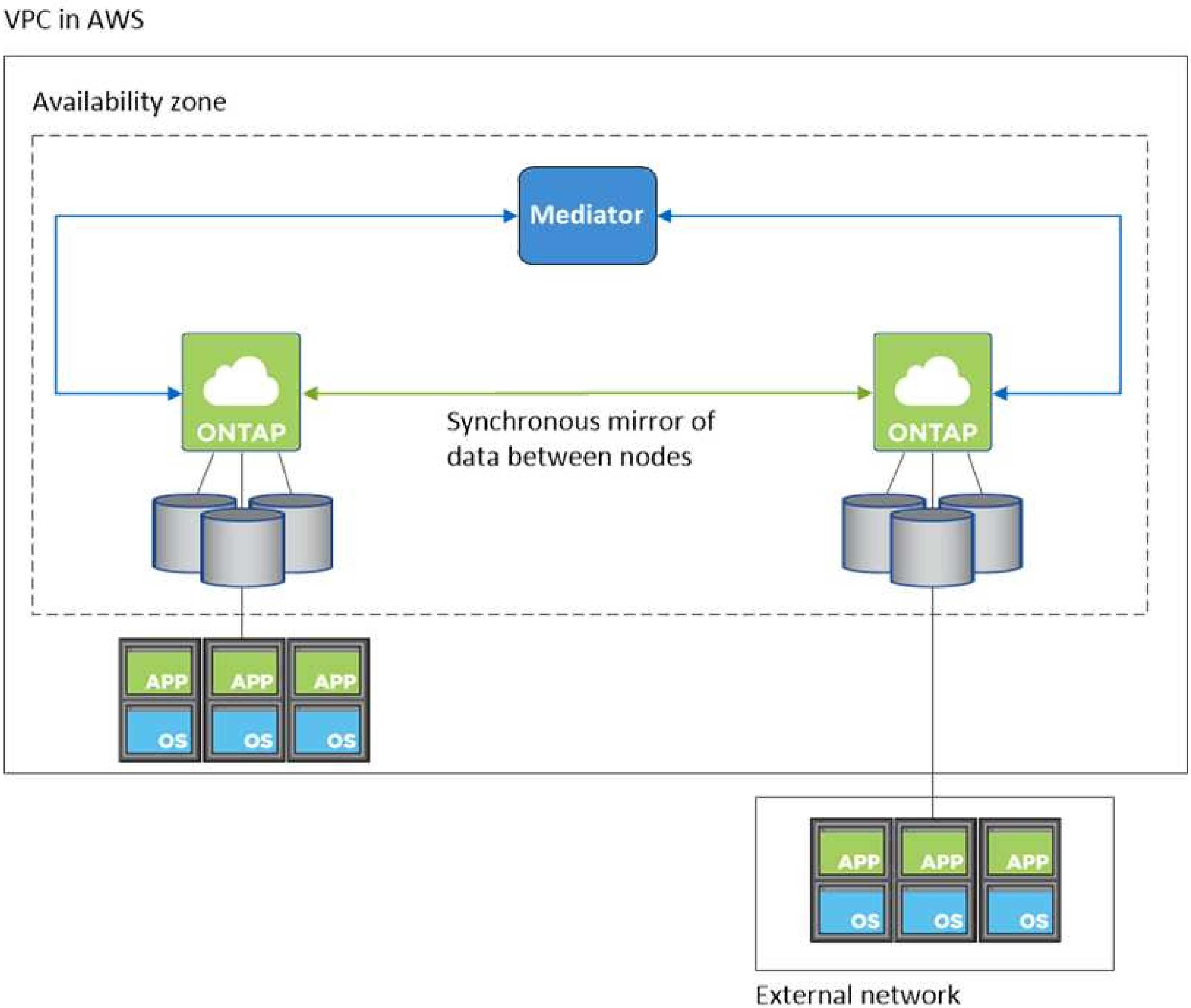
Deploying an HA configuration in a single availability zone (AZ) can ensure high availability of your data if an instance that runs a Cloud Volumes ONTAP node fails. All data is natively accessible from outside of the VPC.

> ⓘ The Console creates an AWS Documentation: AWS spread placement group and launches the two HA nodes in that placement group. The placement group reduces the risk of simultaneous failures by spreading the instances across distinct underlying hardware. This feature improves redundancy from a compute perspective and not from disk failure perspective.

Data access

Because this configuration is in a single AZ, it does not require floating IP addresses. You can use the same IP address for data access from within the VPC and from outside the VPC.

The following image shows an HA configuration in a single AZ. Data is accessible from within the VPC and from outside the VPC.



Takeover and giveback

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, refer to the NetApp Interoperability Matrix Tool and the SAN hosts and cloud clients guide for your host operating system.

For NAS configurations, the data IP addresses can migrate between HA nodes if failures occur. This ensures client access to storage.

AWS Local Zones

AWS Local Zones are an infrastructure deployment where storage, compute, database, and other select AWS services are located close to large cities and industry areas. With AWS Local Zones, you can bring AWS services closer to you which improves latency for your workloads and maintain databases locally. On Cloud Volumes ONTAP, You can deploy a single AZ or multiple AZ configuration in AWS Local Zones.

> AWS Local Zones are supported when using the Console in standard and private modes. At this time, AWS Local Zones are not supported in restricted mode.

Example AWS Local Zone configurations

Cloud Volumes ONTAP in AWS supports only high availability (HA) mode in a single availability zone. Single node deployments are not supported.

Cloud Volumes ONTAP does not support data tiering, cloud tiering, and unqualified instances in AWS Local Zones.

The following are example configurations:

- Single availability zone: Both cluster nodes and the mediator are in the same Local Zone.
- Multiple availability zones
  In multiple availability zone configurations, there are three instances, two nodes and one mediator. One instance out of the three instances must be in a separate zone. You can choose how you set this up.

  Here are three example configurations:

  - Each cluster node is in a different Local Zone and the mediator in a public availability zone.
  - One cluster node in a Local Zone, the mediator in a Local Zone, and the second cluster node is in an availability zone.
  - Each cluster node and the mediator are in separate Local Zones.

Supported disk and instance types

The only supported disk type is GP2. The following EC2 instance type families with sizes xlarge to 4xlarge are currently supported:

- M5
- C5
- C5d
- R5
- R5d

> Cloud Volumes ONTAP supports only these configurations. Selecting unsupported disk types or unqualified instances in AWS Local Zone configuration might result in deployment failure. Data tiering to Amazon Simple Storage Service (Amazon S3) is not supported if your Cloud Volumes ONTAP system is in an AWS Local Zone, because accessing the Amazon S3 buckets outside of the Local Zone involves higher latency and impacts Cloud Volumes ONTAP activities.

AWS Documentation: EC2 instance types in Local Zones.

How storage works in an HA pair

Unlike an ONTAP cluster, storage in a Cloud Volumes ONTAP HA pair is not shared between nodes. Instead, data is synchronously mirrored between the nodes so that the data is available in the event of failure.

Storage allocation

When you create a new volume and additional disks are required, the Console allocates the same number of disks to both nodes, creates a mirrored aggregate, and then creates the new volume. For example, if two disks are required for the volume, the Console allocates two disks per node for a total of four disks.

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.

> You can set up an active-active configuration only when using the Console in the Storage System View.

Performance expectations

A Cloud Volumes ONTAP HA configuration synchronously replicates data between nodes, which consumes network bandwidth. As a result, you can expect the following performance in comparison to a single-node Cloud Volumes ONTAP configuration:

- For HA configurations that serve data from only one node, read performance is comparable to the read performance of a single-node configuration, whereas write performance is lower.
- For HA configurations that serve data from both nodes, read performance is higher than the read performance of a single-node configuration, and write performance is the same or higher.

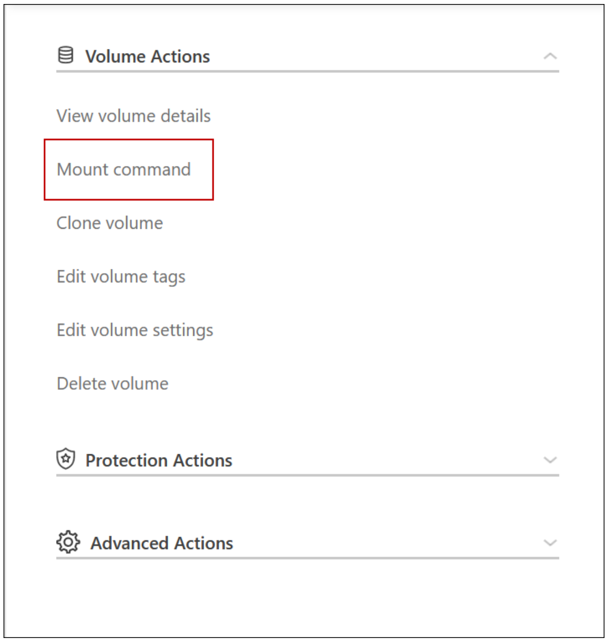
For more details about Cloud Volumes ONTAP performance, refer to Performance.

Client access to storage

Clients should access NFS and CIFS volumes by using the data IP address of the node on which the volume resides. If NAS clients access a volume by using the IP address of the partner node, traffic goes between both nodes, which reduces performance.

> If you move a volume between nodes in an HA pair, you should remount the volume by using the IP address of the other node. Otherwise, you can experience reduced performance. If clients support NFSv4 referrals or folder redirection for CIFS, you can enable those features on the Cloud Volumes ONTAP systems to avoid remounting the volume. For details, refer to the ONTAP documentation.

You can easily identify the correct IP address through the *Mount Command* option under the manage volumes panel in.



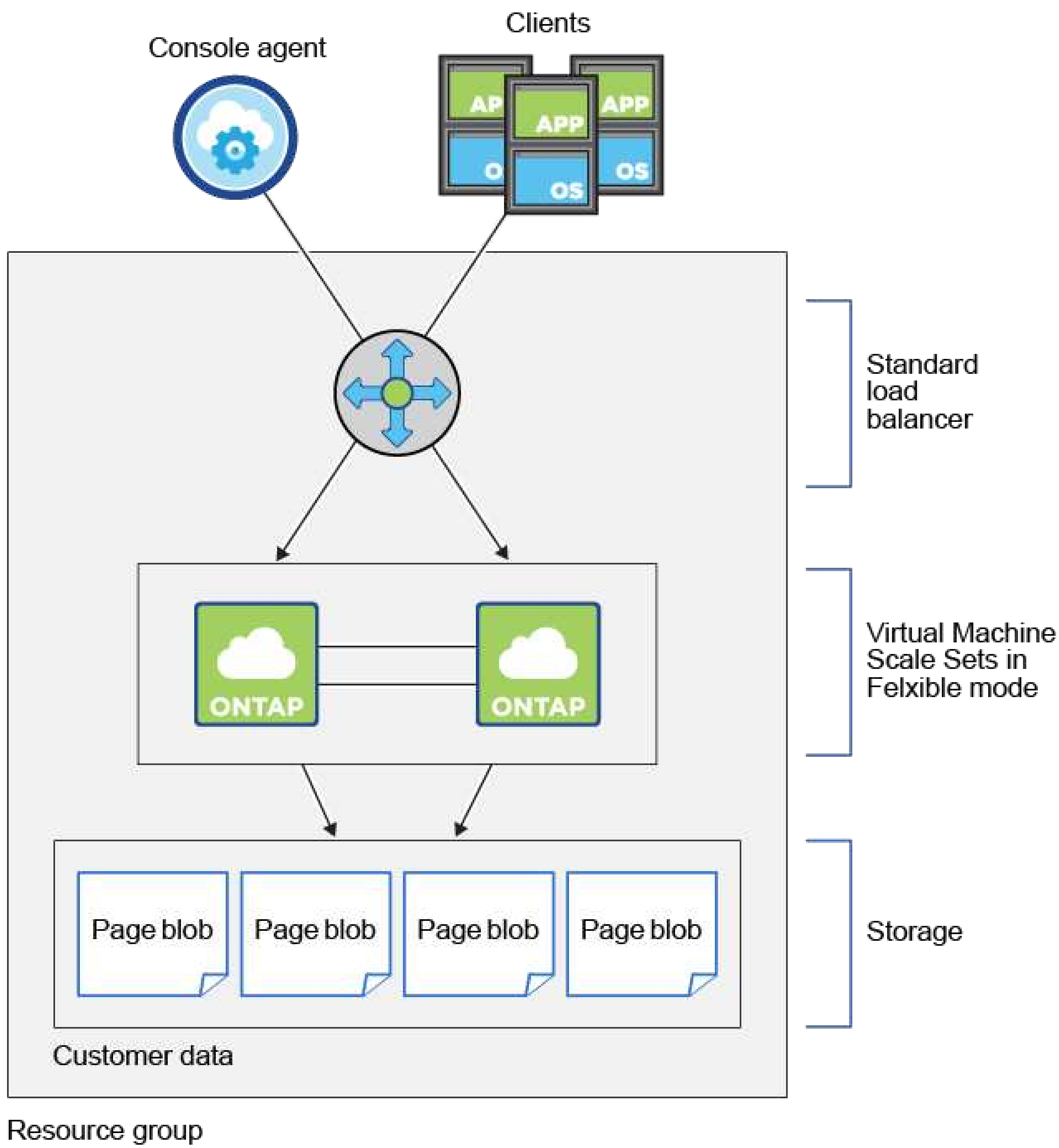
Learn about Cloud Volumes ONTAP HA pairs in Azure

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

HA single availability zone configuration with page blobs

A Cloud Volumes ONTAP HA page blob configuration in Azure includes the following components:



Note the following about the Azure components that the NetApp Console deploys for you:

Azure Standard Load Balancer

The load balancer manages incoming traffic to the Cloud Volumes ONTAP HA pair.

VMs in single availability zones

Beginning with Cloud Volumes ONTAP 9.15.1, you can create and manage heterogeneous virtual machines (VMs) in a single availability zone (AZ). You can deploy high-availability (HA) nodes in separate fault domains within the same AZ, guaranteeing optimal availability. To learn more about the flexible orchestration mode that enables this capability, refer to the Microsoft Azure documentation: Virtual Machine Scale Sets.

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.

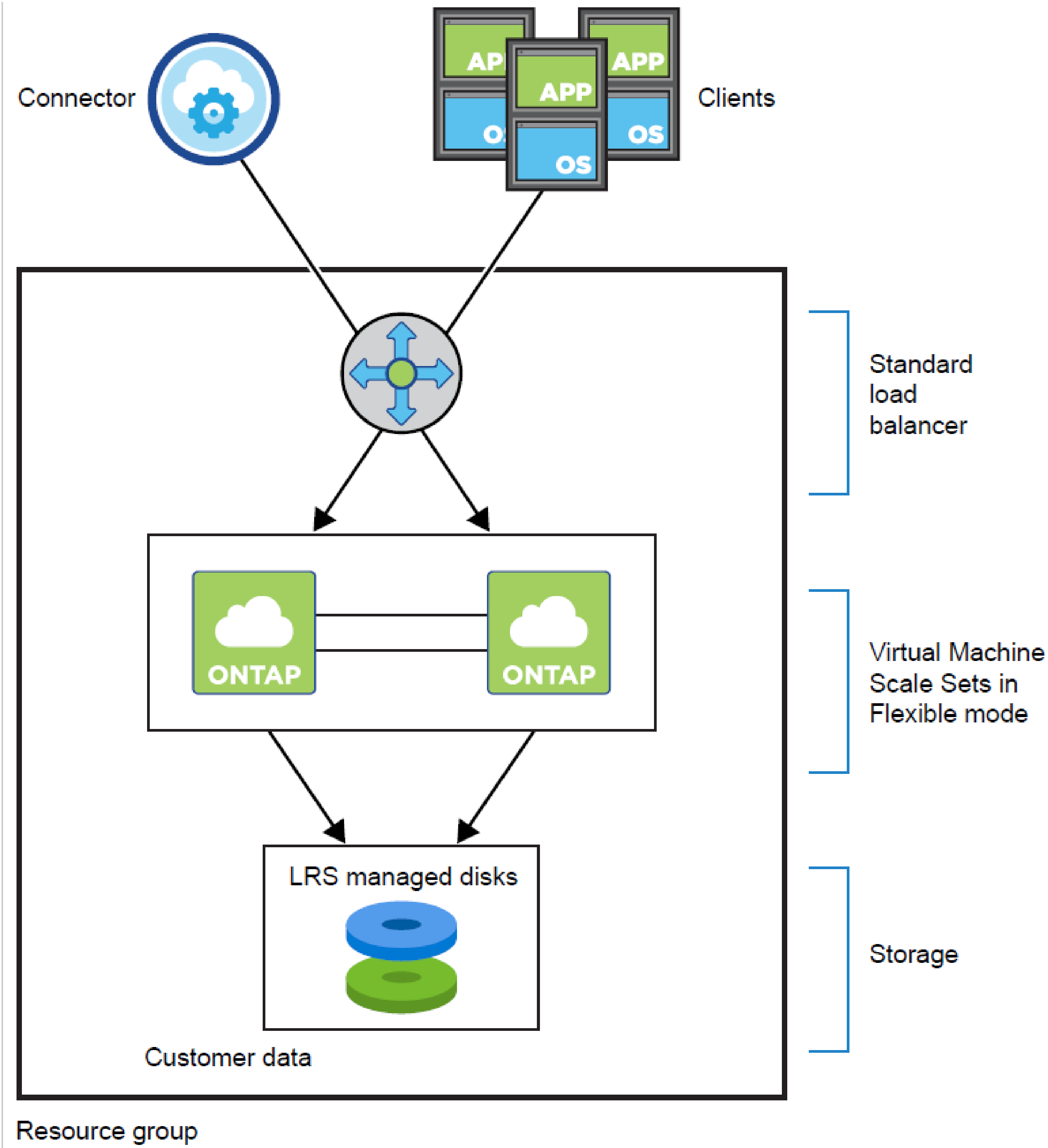
  Microsoft Azure documentation: Azure Storage scalability and performance targets for storage accounts.

- One storage account is required for data tiering to Azure Blob storage.
- Starting with Cloud Volumes ONTAP 9.7, the storage accounts that the Console 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 adding a Cloud Volumes ONTAP system. Note that enabling this option can impact write performance. You can't change the setting after you create the system.

> Starting with Cloud Volumes ONTAP 9.15.0P1, Azure page blobs are no longer supported for new high-availability pair deployments. If you currently use Azure page blobs in existing high-availability pair deployments, you can migrate to newer VM instance types in the Edsv4-series VMs and Edsv5-series VMs.
> Learn more about supported configurations in Azure.

HA single availability zone configuration with shared managed disks

A Cloud Volumes ONTAP HA single availability zone configuration running on top of shared managed disk includes the following components:



Note the following about the Azure components that the Console deploys for you:

Azure Standard Load Balancer

The load balancer manages incoming traffic to the Cloud Volumes ONTAP HA pair.

VMs in single availability zones

Beginning with Cloud Volumes ONTAP 9.15.1, you can create and manage heterogeneous virtual machines (VMs) in a single availability zone (AZ). You can deploy high-availability (HA) nodes in separate fault domains within the same AZ, guaranteeing optimal availability. To learn more about the flexible orchestration mode that enables this capability, refer to the Microsoft Azure documentation: Virtual Machine

Scale Sets.

The zonal deployment uses Premium SSD v2 Managed Disks when the following conditions are fulfilled:

- The version of Cloud Volumes ONTAP is 9.15.1 or later.
- The selected region and zone support Premium SSD v2 Managed Disks. For information about the supported regions, refer to Microsoft Azure website: Products available by region.
- The subscription is registered for the Microsoft Microsoft.Compute/VMOrchestratorZonalMultiFD feature.

> If you choose Premium SSD Managed Disks for an environment that fulfils the above criteria, the Console automatically deploys Premium SSD v2 Managed Disks. You cannot switch to Premium SSD v1 Managed Disks.

Disks

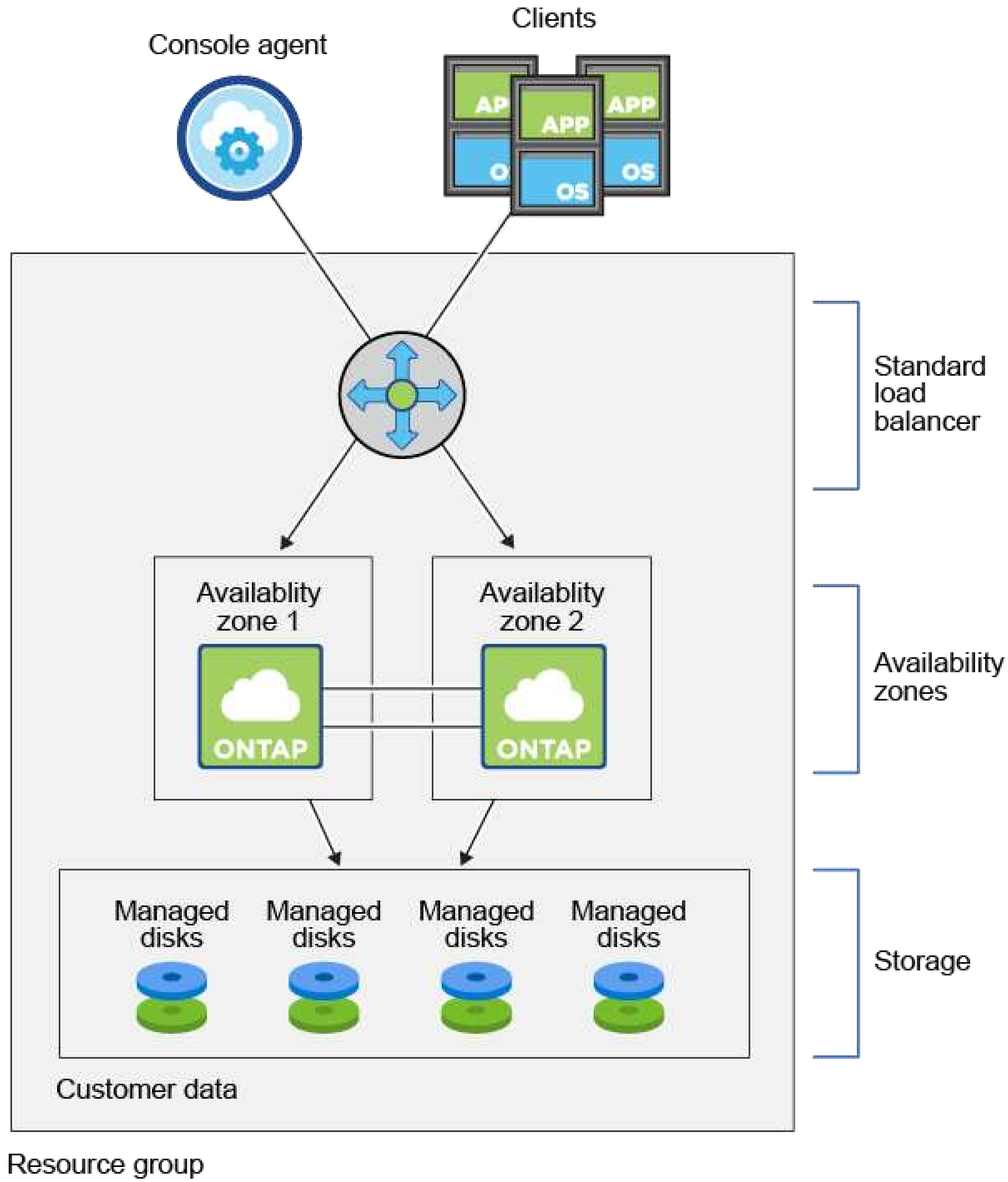
Customer data resides on locally-redundant storage (LRS) managed disks. Each node has access to the other node's storage. Additional storage is also required for boot, root, partner root, core, and NVRAM data.

Storage accounts

Storage accounts are used for managed disk based deployments to handle diagnostic logs and tiering to blob storage.

HA multiple availability zone configuration

A Cloud Volumes ONTAP HA multiple availability zone configuration in Azure includes the following components:



Note the following about the Azure components that the Console deploys for you:

Azure Standard Load Balancer

The load balancer manages incoming traffic to the Cloud Volumes ONTAP HA pair.

Availability Zones

HA multiple availability zone configuration utilizes a deployment model where two Cloud Volumes ONTAP nodes are deployed into different availability zones, ensuring that the nodes are in different fault domains to provide redundancy and availability. To learn how Virtual Machine Scale Sets in Flexible orchestration mode can use availability zones in Azure, refer to the Microsoft Azure documentation: Create a Virtual Machine Scale Set that uses Availability Zones.

Disks

Customer data resides on zone-redundant storage (ZRS) managed disks. Each node has access to the other node's storage. Additional storage is also required for boot, root, partner root, and core data.

Storage accounts

Storage accounts are used for managed disk based deployments to handle diagnostic logs and tiering to blob storage.

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 120 seconds.
  In the event of an outage, data should be available in 120 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, refer to the NetApp Interoperability Matrix Tool and the SAN hosts and cloud clients 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 the storage for the active node.

Learn about Cloud Volumes ONTAP HA pairs in Google Cloud

A Cloud Volumes ONTAP high-availability (HA) configuration provides nondisruptive operations and fault tolerance. In Google Cloud, data is synchronously mirrored between the two nodes.

HA components

Cloud Volumes ONTAP HA configurations in Google Cloud include the following components:

- Two Cloud Volumes ONTAP nodes whose data is synchronously mirrored between each other.

- A mediator instance that provides a communication channel between the nodes to assist in storage takeover and giveback processes.
- One zone or three zones (recommended).

  If you choose three zones, the two nodes and mediator are in separate Google Cloud zones.

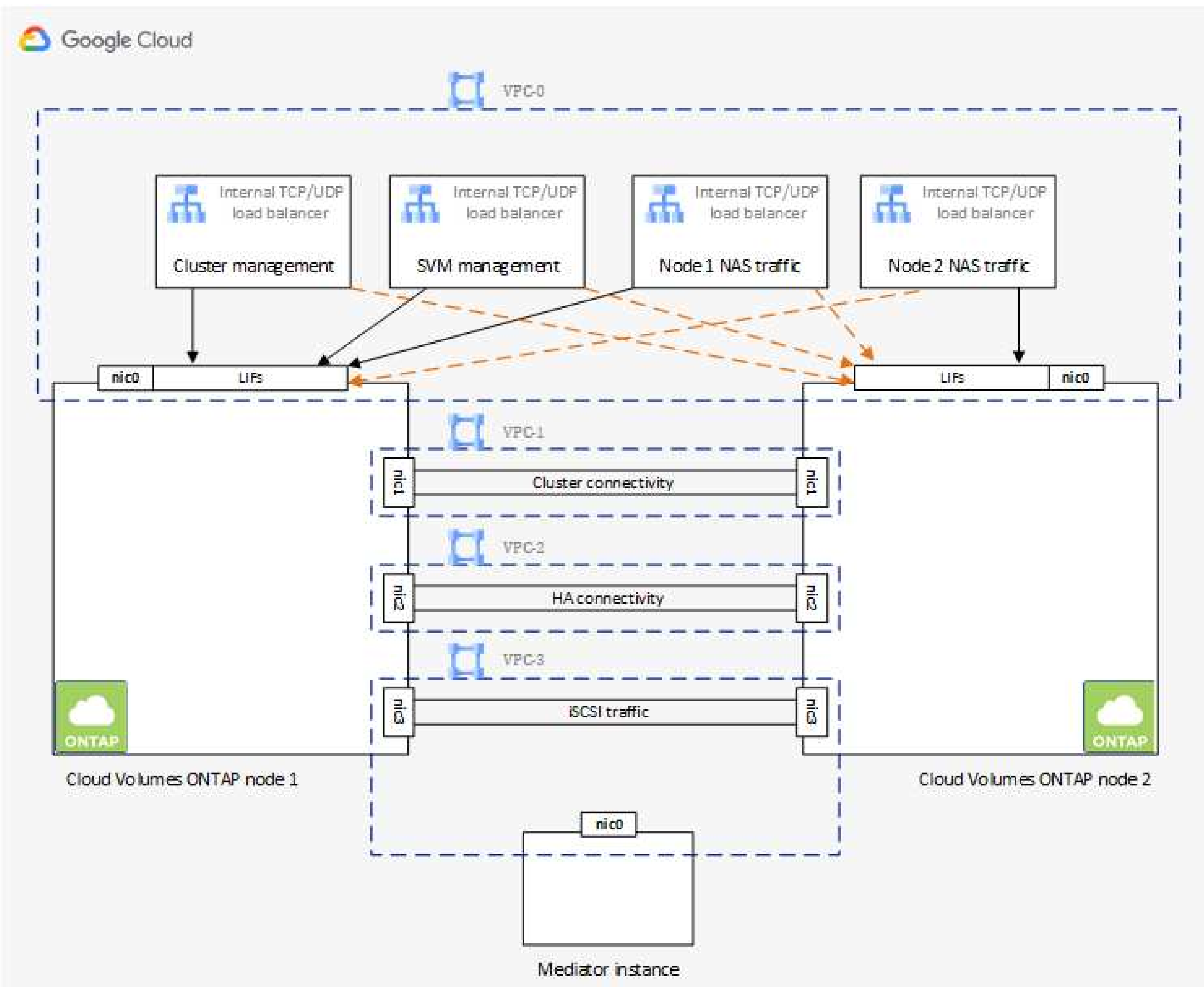
- Four Virtual Private Clouds (VPCs).

  The configuration uses four VPCs because GCP requires that each network interface resides in a separate VPC network.

- Four Google Cloud internal load balancers (TCP/UDP) that manage incoming traffic to the Cloud Volumes ONTAP HA pair.

Learn about networking requirements, including more details about load balancers, VPCs, internal IP addresses, subnets, and more.

The following conceptual image shows a Cloud Volumes ONTAP HA pair and its components:



Mediator

Here are some key details about the mediator instance in Google Cloud:

Instance type
e2-micro (an f1-micro instance was previously used)

Disks
Two standard persistent disks that are 10 GiB each

Operating system
Debian 11

> For Cloud Volumes ONTAP 9.10.0 and earlier, Debian 10 was installed on the mediator.

Upgrades
When you upgrade Cloud Volumes ONTAP, the NetApp Console also updates the mediator instance as needed.

Access to the instance
For Debian, the default cloud user is `admin`. Google Cloud creates and adds a certificates for the `admin` user when SSH access is requested through the Google Cloud Console or gcloud command line. You can specify `sudo` to gain root privileges.

Third-party agents
Third-party agents or VM extensions are not supported on the mediator instance.

Storage takeover and giveback

If a node goes down, the other node can serve data for its partner to provide continued data service. Clients can access the same data from the partner node because the data was synchronously mirrored to the partner.

After the node reboots, the partner must resync data before it can return the storage. The time that it takes to resync data depends on how much data was changed while the node was down.

Storage takeover, resync, and giveback are all automatic by default. No user action is required.

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 120 seconds.

  In the event of an outage, data should be available in 120 seconds or less.

HA deployment models

You can ensure the high availability of your data by deploying an HA configuration in multiple zones or in a single zone.

Multiple zones (recommended)

Deploying an HA configuration across three zones ensures continuous data availability if a failure occurs within a zone. Note that write performance is slightly lower compared to using a single zone, but it's minimal.

Single zone

When deployed in a single zone, a Cloud Volumes ONTAP HA configuration uses a spread placement policy. This policy ensures that an HA configuration is protected from a single point of failure within the zone, without having to use separate zones to achieve fault isolation.

This deployment model does lower your costs because there are no data egress charges between zones.

How storage works in an HA pair

Unlike an ONTAP cluster, storage in a Cloud Volumes ONTAP HA pair in GCP is not shared between nodes. Instead, data is synchronously mirrored between the nodes so that the data is available in the event of failure.

Storage allocation

When you create a new volume and additional disks are required, the Console allocates the same number of disks to both nodes, creates a mirrored aggregate, and then creates the new volume. For example, if two disks are required for the volume, the Console allocates two disks per node for a total of four disks.

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.

Performance expectations for an HA configuration

A Cloud Volumes ONTAP HA configuration synchronously replicates data between nodes, which consumes network bandwidth. As a result, you can expect the following performance in comparison to a single-node Cloud Volumes ONTAP configuration:

- For HA configurations that serve data from only one node, read performance is comparable to the read performance of a single-node configuration, whereas write performance is lower.
- For HA configurations that serve data from both nodes, read performance is higher than the read performance of a single-node configuration, and write performance is the same or higher.

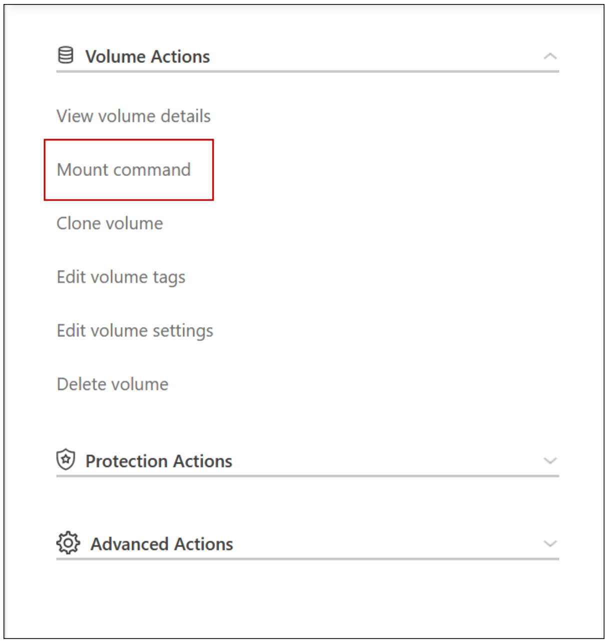
For more details about Cloud Volumes ONTAP performance, refer to Performance.

Client access to storage

Clients should access NFS and CIFS volumes by using the data IP address of the node on which the volume resides. If NAS clients access a volume by using the IP address of the partner node, traffic goes between both nodes, which reduces performance.

> If you move a volume between nodes in an HA pair, you should remount the volume by using the IP address of the other node. Otherwise, you can experience reduced performance. If clients support NFSv4 referrals or folder redirection for CIFS, you can enable those features on the Cloud Volumes ONTAP systems to avoid remounting the volume. For details, refer to ONTAP documentation.

You can locate the correct IP address from the Console by selecting the volume and clicking **Mount Command**.



Related links

- Learn about networking requirements
- Learn how to get started in GCP

Operations unavailable when a node in Cloud Volumes ONTAP HA pair is offline

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 system in the NetApp Console is *Degraded*.

The following actions are unavailable from 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 system changes back to normal.

Learn about Cloud Volumes ONTAP data encryption and ransomware protection

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)
- AWS Key Management Service
- Azure Storage Service Encryption
- Google Cloud Platform default 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.

Cloud Volumes ONTAP supports both NVE and NAE with external key management services (EKMs) provided by AWS, Azure, and Google Cloud, including third-party solutions, such as Fortanix. Unlike ONTAP, for Cloud Volumes ONTAP, encryption keys are generated at the cloud provider's side, not in ONTAP. Cloud Volumes ONTAP doesn't support Onboard Key Manager.

Cloud Volumes ONTAP uses the standard Key Management Interoperability Protocol (KMIP) services that ONTAP uses. For more information about the supported services, refer to the Interoperability Matrix Tool.

If you use NVE, you have the option to use your cloud provider's key vault to protect ONTAP encryption keys:

- AWS Key Management Service (KMS)
- Azure Key Vault (AKV)
- Google Cloud Key Management Service

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 have 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 Encrypt volumes with NetApp encryption solutions.

AWS Key Management Service

When you launch a Cloud Volumes ONTAP system in AWS, you can enable data encryption using the AWS Key Management Service (KMS). The NetApp Console requests data keys using a customer master key (CMK).

> You can't change the AWS data encryption method after you create a Cloud Volumes ONTAP system.

If you want to use this encryption option, then you must ensure that the AWS KMS is set up appropriately. For information, refer to Setting up the AWS KMS.

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.

Google Cloud Platform default encryption

Google Cloud Platform data-at-rest encryption is enabled by default for Cloud Volumes ONTAP. No setup is required.

While Google Cloud Storage always encrypts your data before it's written to disk, you can use the Console APIs to create a Cloud Volumes ONTAP system that uses *customer-managed encryption keys*. These are keys that you generate and manage in GCP using the Cloud Key Management Service. Learn more.

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, refer to the NetApp Interoperability Matrix.

For information about how to configure and manage the antivirus functionality on ONTAP systems, refer to the ONTAP 9 Antivirus Configuration Guide.

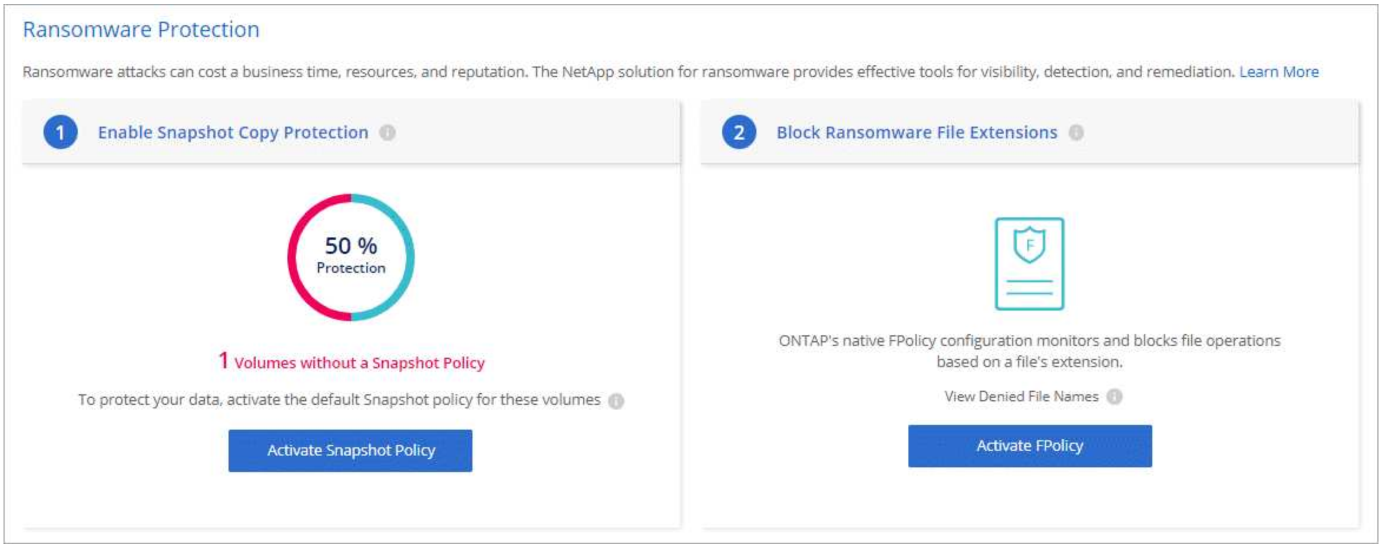
Ransomware protection

Ransomware attacks can cost a business time, resources, and reputation. The Console enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

- The Console 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.

* The Console also enables you to block common ransomware file extensions by enabling ONTAP's FPolicy solution.



Learn how to implement the NetApp solution for ransomware.

Learn about performance monitoring for Cloud Volumes ONTAP workloads

You can review performance results to help you decide which workloads are appropriate for Cloud Volumes ONTAP.

Performance technical reports

* Cloud Volumes ONTAP for AWS

  NetApp Technical Report 4383: Performance Characterization of Cloud Volumes ONTAP in Amazon Web Services with Application Workloads

* Cloud Volumes ONTAP for Microsoft Azure

  NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads

* Cloud Volumes ONTAP for Google Cloud

  NetApp Technical Report 4816: Performance Characterization of Cloud Volumes ONTAP for Google Cloud

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.

For information, refer to the 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 bring your own license (BYOL) must have a system license installed with an active subscription. The NetApp Console simplifies the process by managing licenses for you and by displaying a warning before they expire.

> A node-based license is the previous generation license for Cloud Volumes ONTAP. A node-based license could be procured from NetApp (BYOL) and is available for license renewals, only in specific cases.

Learn more about Cloud Volumes ONTAP licensing options.

Learn more about how to manage node-based licenses.

BYOL system licenses

Node-based licenses could be procured from NetApp. The number of licenses that you can purchase for a single-node system or HA pair is unlimited.

> NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAPP.

A node-based license provides up to 368 TiB of capacity for a single node or HA pair. You might have purchased multiple licenses for a Cloud Volumes ONTAP BYOL system to allocate more than 368 TiB of capacity. For example, you might have two licenses to allocate up to 736 TiB of capacity to Cloud Volumes ONTAP. Or you could have four licenses to get up to 1.4 PiB.

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, the Console prompts you for the serial number of your license and your NetApp Support Site account. The Console 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 the Console.

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

License expiration

The Console 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 system to review the message.

The Console includes a license expiration warning in the Cloud Volumes ONTAP report that's emailed to you, if you are an organization or 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

If you renew a node-based BYOL subscription by contacting a NetApp representative, the Console automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system.

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

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.

Learn how AutoSupport and Digital Advisor are used for Cloud Volumes ONTAP

The AutoSupport component of ONTAP collects telemetry and sends it for analysis. Active IQ Digital Advisor (also known as Digital Advisor) analyzes the data from AutoSupport and provides proactive care and optimization. Using artificial intelligence, Digital Advisor can identify potential problems and help you resolve them before they impact your business.

Digital Advisor 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 Digital Advisor 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 Digital Advisor:

- Plan upgrades.

  Digital Advisor 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 Digital Advisor 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.

  Digital Advisor 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.

  Digital Advisor displays complete inventory and software and hardware configuration information. See when service contracts are expiring and renew them to ensure you remain supported.

Related links

- NetApp Documentation: Digital Advisor
- Launch Digital Advisor
- SupportEdge Services

Supported default configurations 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

- The NetApp Console creates one data-serving storage VM when it deploys Cloud Volumes ONTAP. Some configurations support additional storage VMs. Learn more about managing storage VMs.

  Beginning with the 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. For information about inline storage efficiency features, refer to the knowledge base article KB: What Inline Storage Efficiency features are supported with CVO?

- The Console 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 9.12.1 GA
  - NetApp Volume Encryption (only for bring your own license (BYOL) or registered pay-as-you-go (PAYGO) systems)
  - NFS
  - ONTAP S3

    Starting with Cloud Volumes ONTAP 9.11.0 in AWS

    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
  - An SVM management LIF on HA systems in Google Cloud
  - An SVM management LIF on single-node systems in AWS
  - A node management LIF

    In Google Cloud, this LIF is combined with the intercluster 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 Console agent using HTTP.

  The backups are accessible from http://ipaddress/occm/offboxconfig/ where *ipaddress* is the IP address of the host of the Console agent.

  You can use the backups for reconfiguring your Cloud Volumes ONTAP system. For more information about configuration backups, refer to the ONTAP documentation.

- The Console sets a few volume attributes differently than other management tools (ONTAP System Manager or the ONTAP CLI, for example).

  The following table lists the volume attributes set differently from the defaults:

Attribute	Value that the Console configures
Autosize mode	grow

Attribute	Value that the Console configures
Maximum autosize	1,000 percent The organization or 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

For information about these attributes, refer to ONTAP *volume create* man page.

Internal disks for system data

In addition to the storage for user data, the Console also purchases cloud storage for system data.

AWS

- Three disks per node for boot, root, and core data:
  - 47 GiB io1 disk for boot data
  - 140 GiB gp3 disk for root data
  - 540 GiB gp2 disk for core data
- For HA pairs:
  - Two st1 EBS volumes for the mediator instance, one of approximately 8 GiB as root disk, and one of 4 GiB as data disk
  - One 140 GiB gp3 disk in each node to contain a copy of the root data of the other node

    In some zones, the available EBS disk type can only be gp2.
- One EBS snapshot for each boot disk and root disk

  Snapshots are created automatically upon reboot.
- When you enable data encryption in AWS using the Key Management Service (KMS), the boot and root disks for Cloud Volumes ONTAP are encrypted, as well. This includes the boot disk for the mediator instance in an HA pair. The disks are encrypted using the CMK that you select when you add a Cloud Volumes ONTAP system.

In AWS, NVRAM is on the boot disk.

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
- Every disk by default in Azure is encrypted at rest.

  If the virtual machine that you chose for Cloud Volumes ONTAP supports Premium SSD v2 Managed Disk as data disks, the system uses a 32 GiB Premium SSD v2 Managed Disk for NVRAM, and another one as the root disk.

Azure (HA pair)

HA pairs with page blob

- 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

  > Snapshots are created automatically upon reboot.
- Every disk by default in Azure is encrypted at rest.

HA pairs with shared managed disks in multiple availability zones

- Two 10 GiB Premium SSD disks for the boot volume (one per node)
- Two 512 GiB Premium SSD disks 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

  > Snapshots are created automatically upon reboot.
- Every disk by default in Azure is encrypted at rest.

HA pairs with shared managed disks in single availability zones

- Two 10 GiB Premium SSD disks for the boot volume (one per node)
- Two 512 GiB Premium SSD Shared Managed disks for the root volume (one per node)
- Two 1024 GiB Standard HDD disks for saving cores (one per node)

* Two 512 GiB Premium SSD Managed disks for NVRAM (one per node)

If your virtual machine supports Premium SSD v2 Managed Disks as data disks, it uses 32 GiB Premium SSD v2 Managed Disks for NVRAM and 512 GiB Premium SSD v2 Shared Managed disks for the root volume.

You can deploy HA pairs in a single single availability zone and use Premium SSD v2 Managed Disks when the following conditions are fulfilled:

* The version of Cloud Volumes ONTAP is 9.15.1 or later.
* The selected region and zone support Premium SSD v2 Managed Disks. For information about the supported regions, refer to Microsoft Azure website: Products available by region.
* The subscription is registered for the Microsoft Microsoft.Compute/VMOrchestratorZonalMultiFD feature.

Google Cloud (single node)

* One 10 GiB SSD persistent disk for boot data
* One 64 GiB SSD persistent disk for root data
* One 500 GiB SSD persistent disk for NVRAM
* One 315 GiB Standard persistent disk for saving cores
* Snapshots for boot and root data

    Snapshots are created automatically upon reboot.

* Boot and root disks are encrypted by default.

Google Cloud (HA pair)

* Two 10 GiB SSD persistent disks for boot data
* Four 64 GiB SSD persistent disk for root data
* Two 500 GiB SSD persistent disk for NVRAM
* Two 315 GiB Standard persistent disk for saving cores
* One 10 GiB Standard persistent disk for mediator data
* One 10 GiB Standard persistent disk for mediator boot data
* Snapshots for boot and root data

    Snapshots are created automatically upon reboot.

* Boot and root disks are encrypted by default.

Where the disks reside

Storage layout:

* 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

Support registration is required to receive technical support specific to the NetApp Console and its storage solutions and data services. Support registration is also required to enable key workflows for Cloud Volumes ONTAP systems.

Registering for support does not enable NetApp support for a cloud provider file service. For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Google Cloud NetApp Volumes

Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your NetApp Console account serial number (your 20 digit 960xxxxxxxxx serial number located on the Support Resources page in the Console).

  This serves as your single support subscription ID for any service within the Console. Each Console account 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 the NetApp Console at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets and automatic case generation. Registration is completed by adding NetApp Support Site (NSS) accounts to the Console as described below.

Register NetApp Console for NetApp support

To register for support and activate support entitlement, one user in your NetApp Console account must associate a NetApp Support Site account with their Console login. 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 the Console.

Steps

1. Select **Administration** > **Credentials**.
2. Select **User Credentials**.

3. Select **Add NSS credentials** and follow the NetApp Support Site (NSS) authentication prompt.
4. To confirm that the registration process was successful, select the Help icon, and select **Support**.

   The **Resources** page should show that your Console account is registered for support.

   Note that other Console users will not see this same support registration status if they have not associated a NetApp Support Site account with their login. However, that doesn't mean that your account is not registered for support. As long as one user in the organization has followed these steps, then your account has been registered.

Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you need to create an NSS account and associate it with your Console login.

Steps

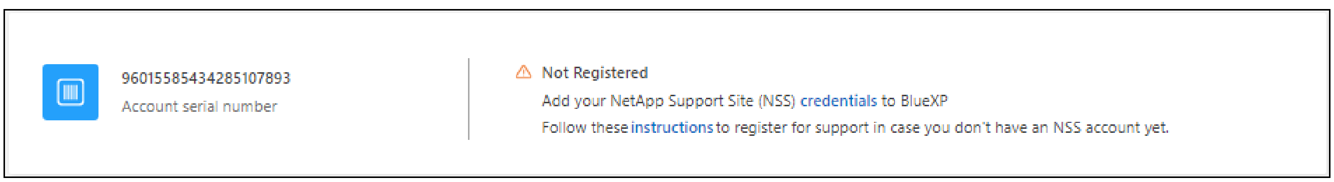
1. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the Console account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.
2. Associate your new NSS account with your Console login by completing the steps under Existing customer with an NSS account.

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 Console, select the Help icon, and select **Support**.
2. Locate your 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 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 account serial number (960xxxx) used above for the serial number field. This will speed up 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, associate the account with your Console login by completing the steps under Existing customer with an NSS account.

Associate NSS credentials for Cloud Volumes ONTAP support

Associating NetApp Support Site credentials with your Console account is required to enable the following key workflows for Cloud Volumes ONTAP:

- Registering pay-as-you-go Cloud Volumes ONTAP systems for support

  Providing your NSS account is required to activate support for your system and to gain access to NetApp technical support resources.

- Deploying Cloud Volumes ONTAP when you bring your own license (BYOL)

  Providing your NSS account is required so that the Console can upload your license key and to enable the subscription for the term that you purchased. This includes automatic updates for term renewals.

- Upgrading Cloud Volumes ONTAP software to the latest release

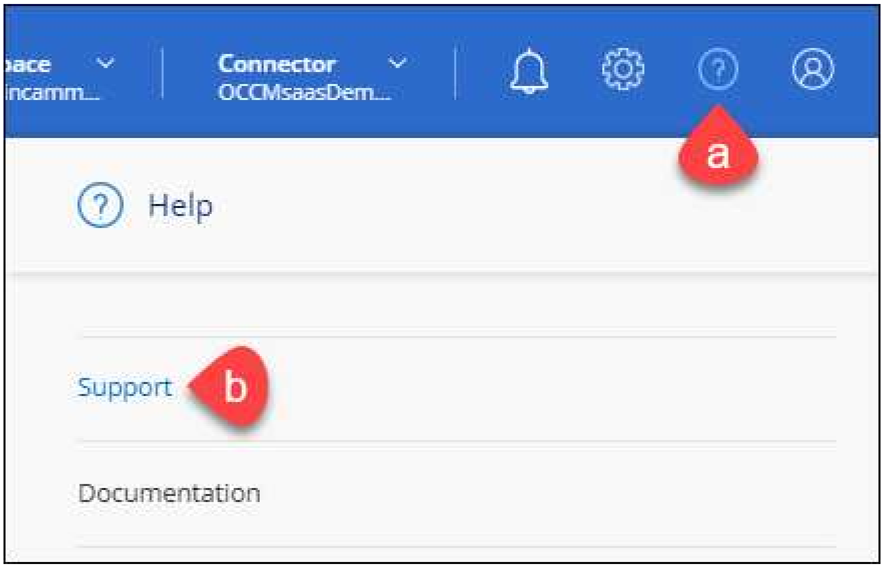
Associating NSS credentials with your NetApp Console account is different than the NSS account that is associated with a Console user login.

These NSS credentials are associated with your specific Console account ID. Users who belong to the Console organization can access these credentials from **Support > NSS Management**.

- 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 Console, select the Help icon, and select **Support**.



2. Select **NSS Management > Add NSS Account**.
3. When you're prompted, select **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Entra ID 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 the Console to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

   Note the following:

   ◦ The NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
   ◦ There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

     "The NSS customer type is not allowed for this account as there are already NSS Users of different type."

     The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level 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. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

Get help

NetApp provides support for NetApp Console and its cloud services in a variety of ways. Extensive free self-support options are available 24/7, such as knowledge base (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Get support for a cloud provider file service

For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to the documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Google Cloud NetApp Volumes

To receive technical support specific to NetApp and its storage solutions and data services, use the support options described below.

Use self-support options

These options are available for free, 24 hours a day, 7 days a week:

- Documentation

  The NetApp Console documentation that you're currently viewing.

- Knowledge base

  Search through the NetApp knowledge base to find helpful articles to troubleshoot issues.

- Communities

  Join the NetApp Console community to follow ongoing discussions or create new ones.

Create a case with 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 associate your NetApp Support Site credentials with your Console login. Learn how to manage credentials associated with your Console login.
- If you're opening a case for an ONTAP system that has a serial number, then your NSS account must be associated with the serial number for that system.

Steps

1. In NetApp Console, select **Help > Support**.
2. On the **Resources** page, choose one of the available options under Technical Support:

a. Select **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. Select **Create a Case** to open a ticket with a NetApp Support specialist:

   - **Service**: Select the service that the issue is associated with. For example, **NetApp Console** when specific to a technical support issue with workflows or functionality within the Console.
   - **System**: If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.

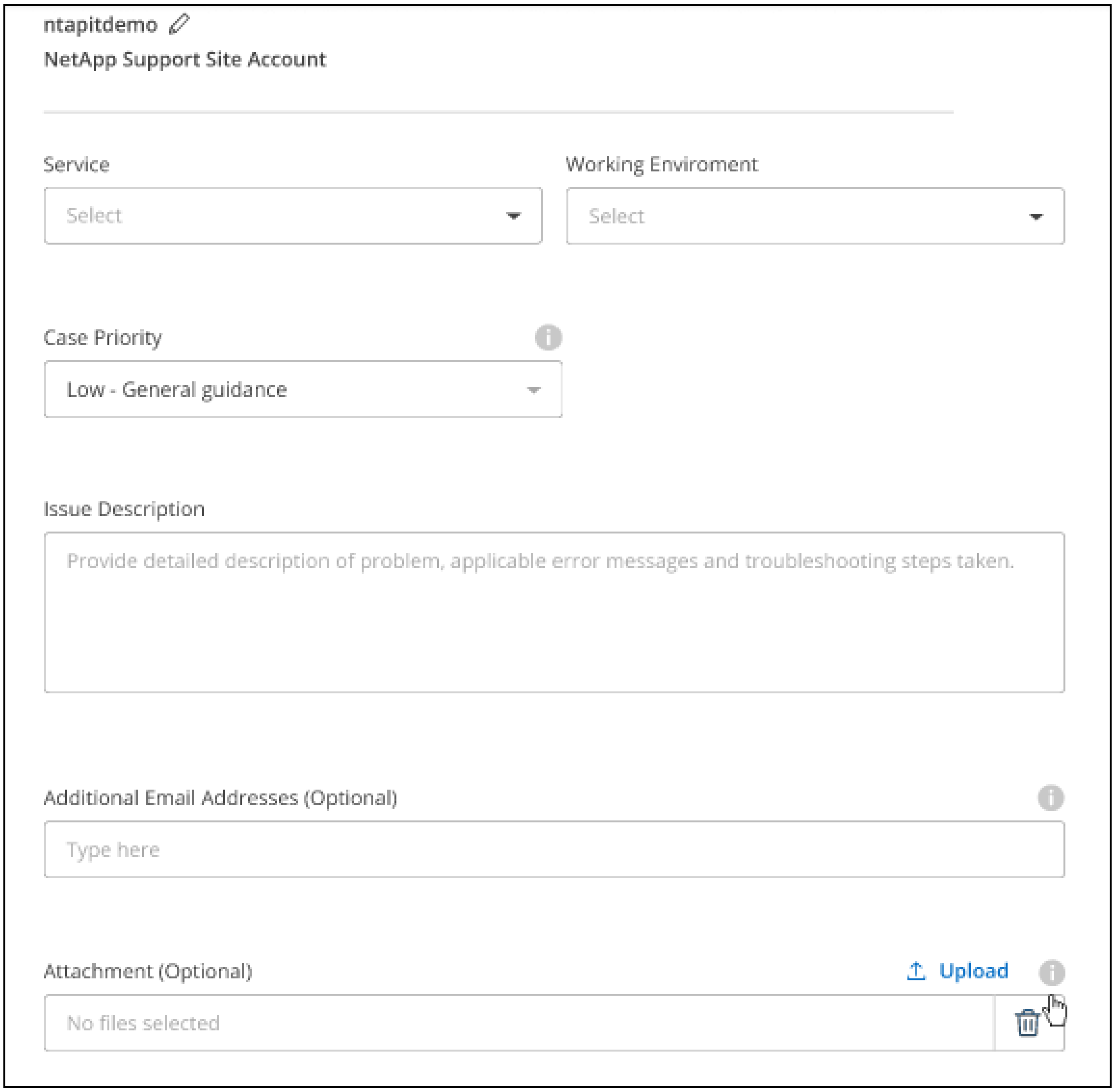
     The list of systems are within scope of the Console organization, and Console agent you have selected in the top banner.

   - **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.
   - **Attachment (Optional)**: Upload up to five attachments, one at a time.

     Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.



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 select **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 NetApp Console account serial number (ie. 960xxxx) or the working environment serial number. You can seek assistance using one of the following options:

- Submit a non-technical case at https://mysupport.netapp.com/site/help

Manage your support cases

You can view and manage active and resolved support cases directly from the Console. You can manage the cases associated with your NSS account and with your company.

Note the following:

- The case management dashboard at the top of the page offers two views:
  - The view on the left shows the total cases opened in the past 3 months by the user NSS account you provided.
  - The view on the right shows the total cases opened in the past 3 months at your company level based on your user NSS account.

  The results in the table reflect the cases related to the view that you selected.

- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

  View the steps below for more details.

- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

Steps

1. In the NetApp Console, select **Help > Support**.
2. Select **Case Management** and if you’re prompted, add your NSS account to the Console.

   The **Case management** page shows open cases related to the NSS account that is associated with your Console user account. This is the same NSS account that appears at the top of the **NSS management** page.

3. Optionally modify the information that displays in the table:
   - Under **Organization’s cases**, select **View** to view all cases associated with your company.
   - Modify the date range by choosing an exact date range or by choosing a different time frame.
   - Filter the contents of the columns.
   - Change the columns that appear in the table by selecting and then choosing the columns that you’d like to display.
4. Manage an existing case by selecting and selecting one of the available options:
   - **View case**: View full details about a specific case.
   - **Update case notes**: Provide additional details about your problem or select **Upload files** to attach up to a maximum of five files.

     Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

   - **Close case**: Provide details about why you’re closing the case and select **Close case**.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

https://www.netapp.com/company/legal/copyright/

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.

https://www.netapp.com/company/legal/trademarks/

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Privacy policy

https://www.netapp.com/company/legal/privacy-policy/

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- Notice for NetApp Console
- Notice for the Cloud Volumes ONTAP
- Notice for ONTAP