



Cloud Volumes ONTAP documentation

Cloud Volumes ONTAP

NetApp
September 04, 2025

This PDF was generated from <https://docs.netapp.com/us-en/blurx-cloud-volumes-ontap/azure/index.html> on September 04, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Cloud Volumes ONTAP documentation	1
Release notes	2
What's new in Cloud Volumes ONTAP	2
4 September 2025	2
11 August 2025	2
14 July 2025	2
25 June 2025	3
29 May 2025	3
12 May 2025	3
16 April 2025	3
14 April 2025	4
3 April 2025	4
28 March 2025	4
12 March 2025	4
10 March 2025	5
6 March 2025	5
03 March 2025	5
18 February 2025	5
10 February 2025	5
9 December 2024	6
11 November 2024	6
25 October 2024	7
7 October 2024	8
9 September 2024	8
23 August 2024	8
22 August 2024	9
8 August 2024	9
10 June 2024	9
17 May 2024	9
23 April 2024	10
8 March 2024	10
5 March 2024	10
2 February 2024	11
16 January 2024	11
8 January 2024	11
6 December 2023	11
5 December 2023	12
10 November 2023	12
8 November 2023	12
1 November 2023	13
23 October 2023	13
6 October 2023	13
10 September 2023	14

30 July 2023	14
26 July 2023	14
2 July 2023	15
26 June 2023	15
4 June 2023	15
7 May 2023	15
4 April 2023	16
3 April 2023	16
13 March 2023	18
5 March 2023	18
5 February 2023	19
1 January 2023	20
15 December 2022	20
8 December 2022	20
4 December 2022	20
15 November 2022	21
6 November 2022	21
18 September 2022	21
31 July 2022	22
18 July 2022	23
3 July 2022	24
7 June 2022	25
2 May 2022	26
3 April 2022	28
27 February 2022	28
9 February 2022	29
6 February 2022	29
30 January 2022	29
2 January 2022	30
28 November 2021	31
4 October 2021	32
2 September 2021	32
7 July 2021	33
30 May 2021	35
24 May 2021	36
11 Apr 2021	36
8 Mar 2021	36
4 Jan 2021	37
3 Nov 2020	39
Known limitations	39
BlueXP doesn't support FlexGroup volumes creation	39
BlueXP doesn't support S3 with Cloud Volumes ONTAP	39
BlueXP doesn't support disaster recovery for storage VMs	39
Cloud Volumes ONTAP Release Notes	40
Get started	41

Learn about Cloud Volumes ONTAP	41
Supported ONTAP versions for Cloud Volumes ONTAP deployments	42
Azure	42
Get started in Microsoft Azure	43
Learn about Cloud Volumes ONTAP deployment options in Azure	43
Get started in BlueXP	44
Deploy Cloud Volumes ONTAP from the Azure marketplace	93
Use Cloud Volumes ONTAP	97
License management	97
Manage capacity-based licensing for Cloud Volumes ONTAP	97
Manage Keystone subscriptions through BlueXP	102
Manage node-based licensing for Cloud Volumes ONTAP	105
Volume and LUN administration	110
Create a FlexVol volume on a Cloud Volumes ONTAP system	110
Manage volumes on Cloud Volumes ONTAP systems	116
Tier inactive Cloud Volumes ONTAP data to a low-cost object storage	125
Connect to a LUN on Cloud Volumes ONTAP from your host system	131
Accelerate data access with FlexCache volumes on a Cloud Volumes ONTAP system	132
Aggregate administration	134
Create an aggregate for Cloud Volumes ONTAP systems	134
Manage aggregates for Cloud Volumes ONTAP clusters	134
Manage the Cloud Volumes ONTAP aggregate capacity on a Connector	135
Storage VM administration	137
Manage storage VMs for Cloud Volumes ONTAP	137
Manage data-serving storage VMs for Cloud Volumes ONTAP in Azure	139
Set up storage VM disaster recovery for Cloud Volumes ONTAP	141
Security and data encryption	141
Encrypt volumes on Cloud Volumes ONTAP with NetApp encryption solutions	142
Manage Cloud Volumes ONTAP encryption keys with Azure Key Vault	142
Enable NetApp ransomware protection solutions for Cloud Volumes ONTAP	150
Create tamperproof Snapshot copies of WORM files on Cloud Volumes ONTAP	153
System administration	154
Upgrade Cloud Volumes ONTAP software	154
Register Cloud Volumes ONTAP pay-as-you-go systems	163
Convert a Cloud Volumes ONTAP node-based license to a capacity-based license	163
Start and stop a Cloud Volumes ONTAP system	166
Synchronize Cloud Volumes ONTAP system time using the NTP server	169
Modify system write speed	169
Change the Cloud Volumes ONTAP cluster admin password	170
Add, remove, or delete systems	171
Azure administration	174
Administer Cloud Volumes ONTAP using System Manager	186
Administer Cloud Volumes ONTAP from the CLI	188
System health and events	189
Verify AutoSupport setup for Cloud Volumes ONTAP	189

Configure EMS for Cloud Volumes ONTAP systems	193
Concepts	194
Licensing	194
Licensing for Cloud Volumes ONTAP	194
Learn more about capacity-based licenses for Cloud Volumes ONTAP	198
Storage	202
Supported client protocols for Cloud Volumes ONTAP	202
Disks and aggregates used for Cloud Volumes ONTAP clusters	203
Learn about data tiering with Cloud Volumes ONTAP in AWS, Azure, or Google Cloud	204
Cloud Volumes ONTAP storage management	207
Write speed	209
Flash Cache	211
Learn about WORM storage on Cloud Volumes ONTAP	212
High-availability pairs	214
Learn about Cloud Volumes ONTAP HA pairs in Azure	214
Operations unavailable when a node in Cloud Volumes ONTAP HA pair is offline	220
Learn about Cloud Volumes ONTAP data encryption and ransomware protection	221
Encryption of data at rest	221
ONTAP virus scanning	222
Ransomware protection	222
Learn about performance monitoring for Cloud Volumes ONTAP workloads	223
Performance technical reports	223
CPU performance	223
License management for node-based BYOL	223
BYOL system licenses	224
License management for a new system	224
License expiration	224
License renewal	225
License transfer to a new system	225
Learn how AutoSupport and Digital Advisor are used for Cloud Volumes ONTAP	226
Supported default configurations for Cloud Volumes ONTAP	227
Default setup	227
Internal disks for system data	228
Knowledge and support	231
Register for support	231
Support registration overview	231
Register BlueXP for NetApp support	231
Associate NSS credentials for Cloud Volumes ONTAP support	233
Get help	235
Get support for a cloud provider file service	235
Use self-support options	235
Create a case with NetApp support	235
Manage your support cases (Preview)	238
Legal notices	241
Copyright	241

Trademarks	241
Patents	241
Privacy policy	241
Open source	241

Cloud Volumes ONTAP documentation

Release notes

What's new in Cloud Volumes ONTAP

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

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

4 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](#)

3 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. After you have deployed Cloud Volumes ONTAP 9.13.1, you can upgrade it to later versions. 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](#)

6 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 **Governance > Digital wallet > 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.](#)

9 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](#).

7 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](#)

9 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.](#)

8 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.

8 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](#).

5 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.](#)

2 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](#)

8 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](#)

6 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](#)

5 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](#).

8 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](#).

1 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](#).

6 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.](#)

2 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.](#)

4 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](#).

7 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."

4 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.

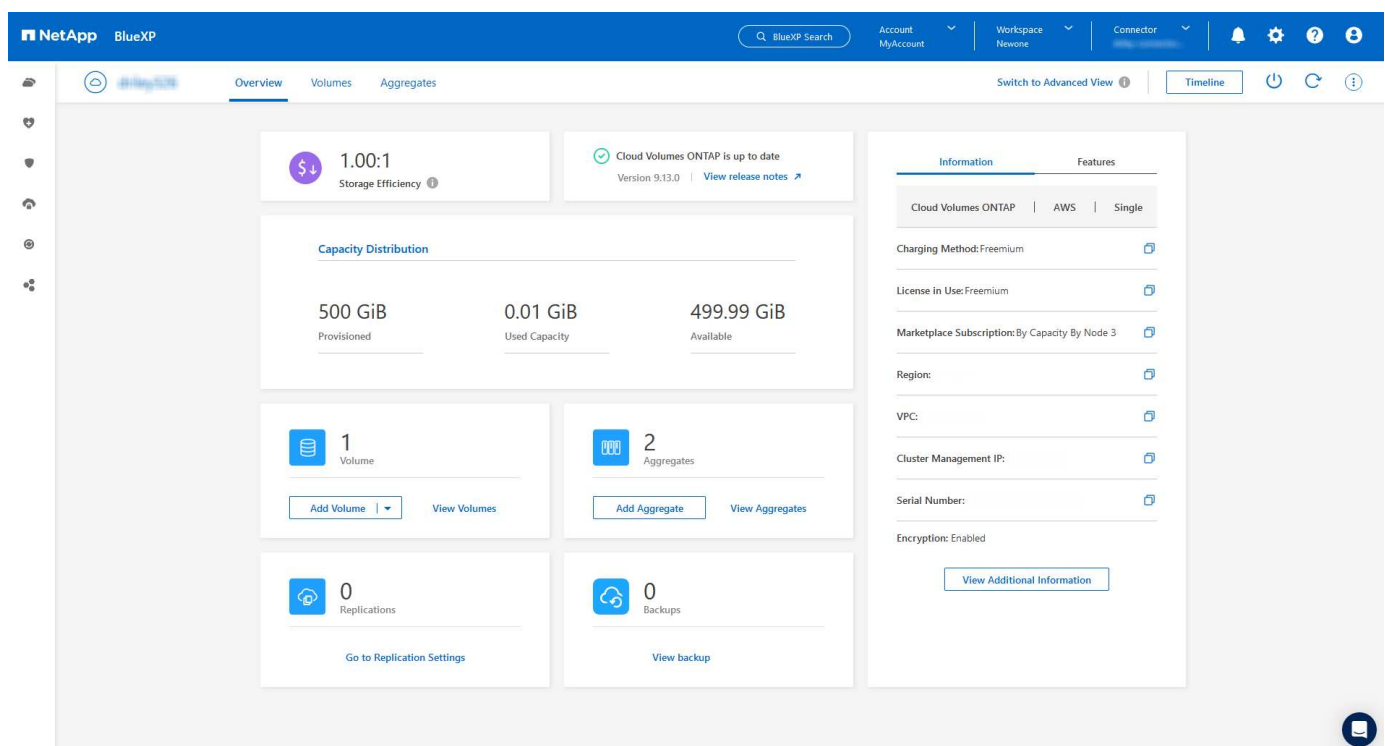
[Learn how to view the consumed capacity in your account.](#)

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.

FlexGroup Volume






Volume

ONLINE

Manage Volume

INFO

Disk Type	GP3
Storage VM	svm_name
Tiering Policy	Snapshot only
Tags	3
Protection	  

CAPACITY

Provisioned	150 TiB
EBS Used	40.2 TiB
S3 Used	26.3 TiB

[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](#).

5 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](#).

5 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.](#)

8 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](#)

4 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](#)

6 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.](#)

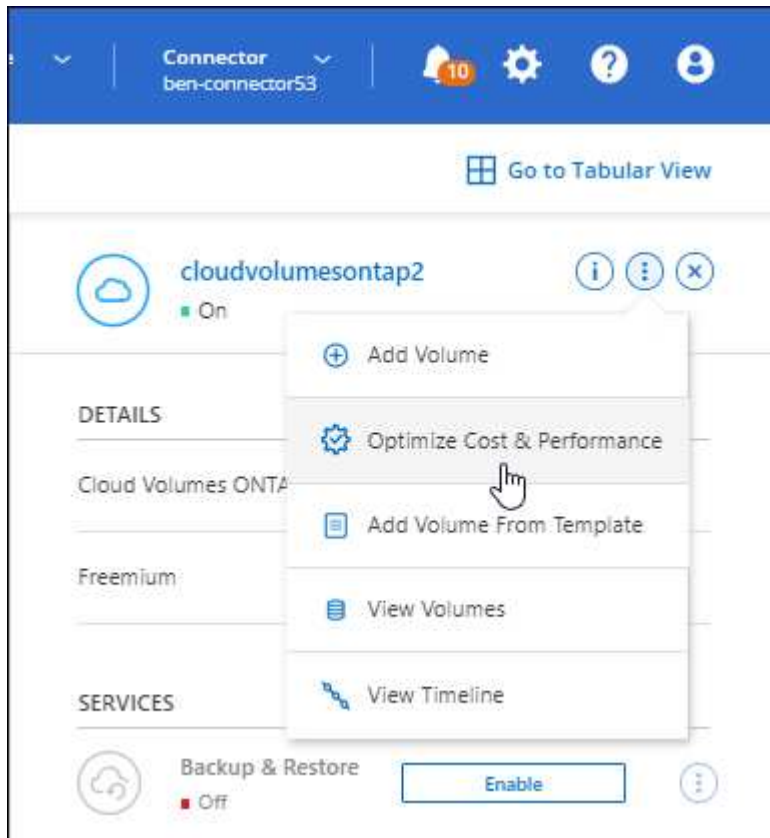
- You can now change from one charging method to the Optimized charging method.

[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.



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.

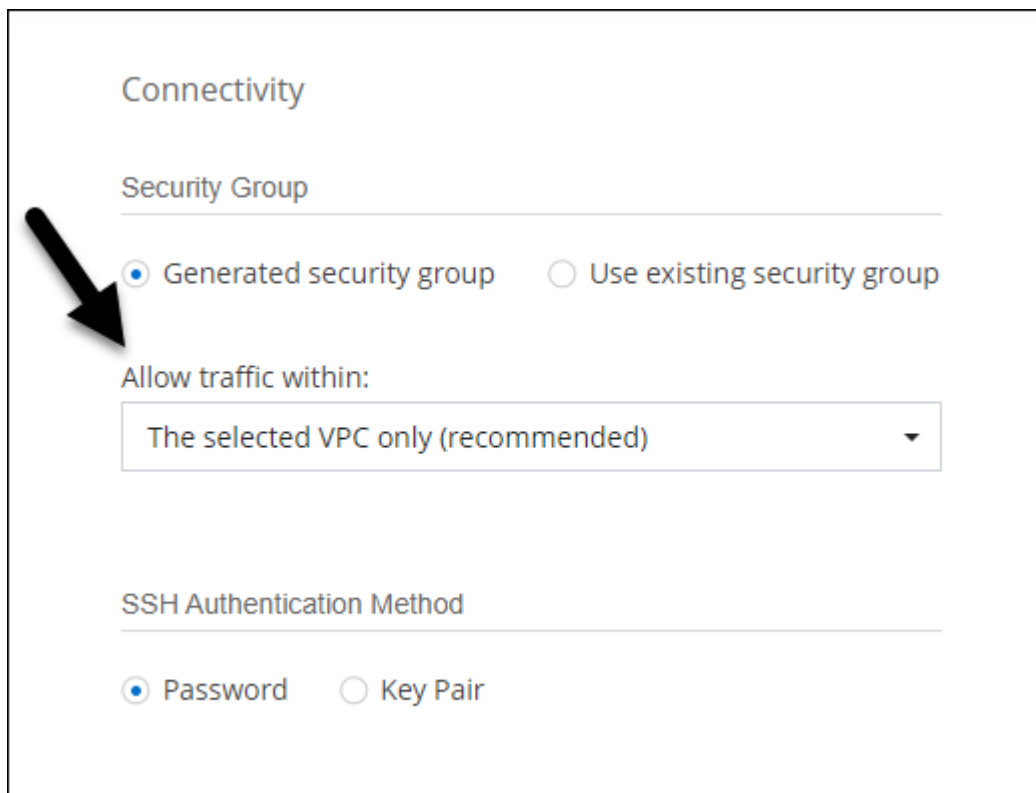
Change charging method

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.



Connectivity

Security Group

☒ Generated security group ☐ Use existing security group

Allow traffic within:

The selected VPC only (recommended) ▼

SSH Authentication Method

☒ Password ☐ Key Pair

18 July 2022

New licensing packages in Azure

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

- **Optimized:** Pay for provisioned capacity and I/O operations separately
- **Edge Cache:** Licensing for [Cloud Volumes Edge Cache](#)

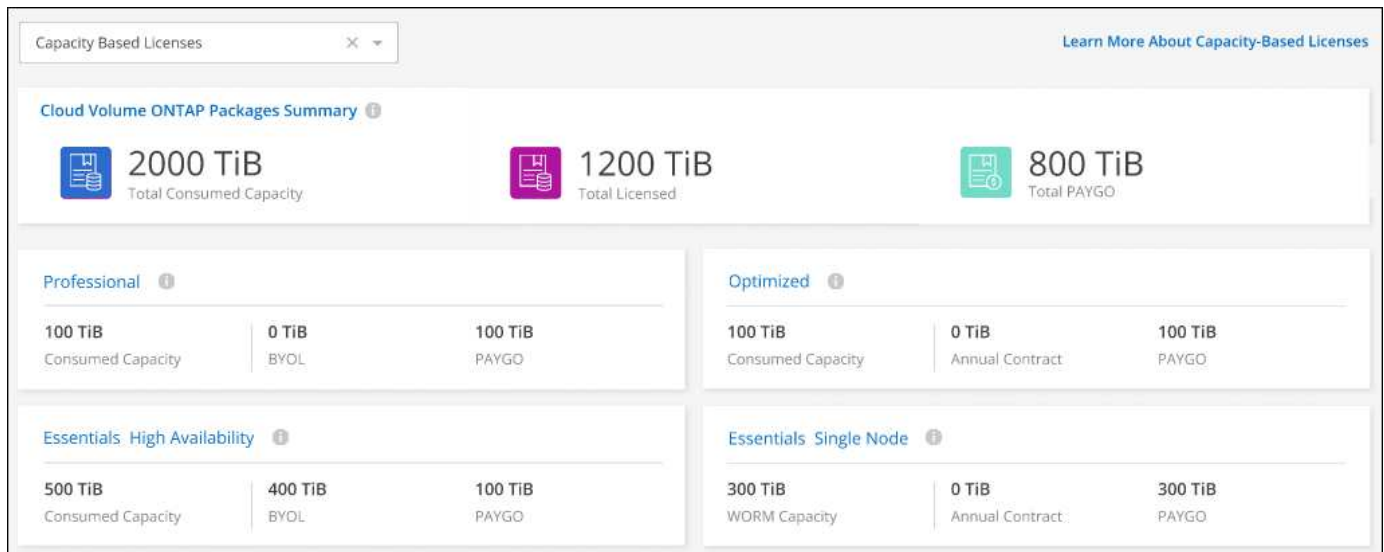
[Learn more about these licensing packages.](#)

3 July 2022

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

Digital Wallet

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



Elastic Volumes enhancement

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](#)

7 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](#)

2 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 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

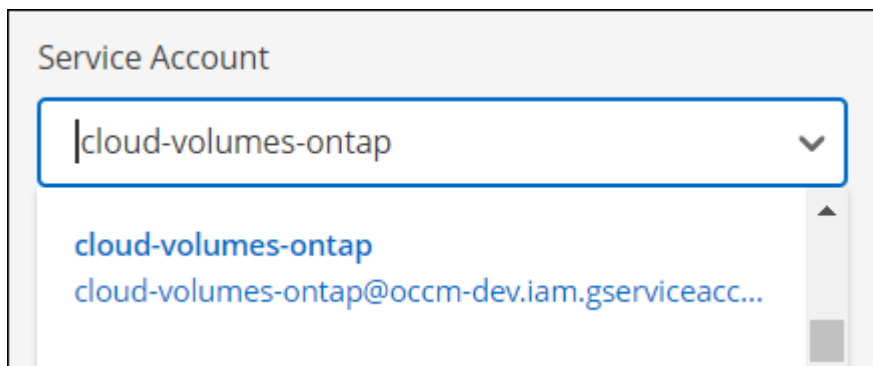
- When you create a Cloud Volumes ONTAP HA pair in Google Cloud, BlueXP will now display all existing firewall policies in a VPC.

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.



3 April 2022

System Manager link has been removed

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

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

Charging for WORM storage

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

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

27 February 2022

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

Redesigned volume wizard

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

[Learn how to create volumes on a specific aggregate.](#)

9 February 2022

Marketplace updates

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

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

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

If you're a new customer, 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.](#)

6 February 2022

Exchange unassigned licenses

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

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

[Learn how to exchange unassigned node-based licenses.](#)

30 January 2022

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

Redesigned licensing selection

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

Digital Wallet update

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

2 January 2022

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

Support for additional Azure VM types

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

- E4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

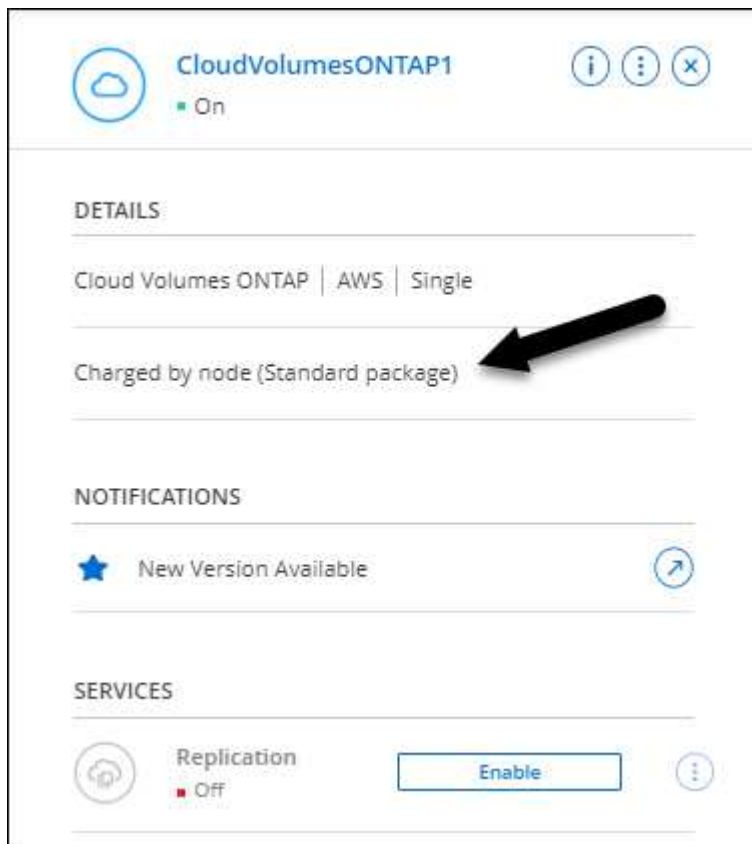
Go to the [Cloud Volumes ONTAP Release Notes](#) for more details about supported configurations.

FlexClone charging update

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

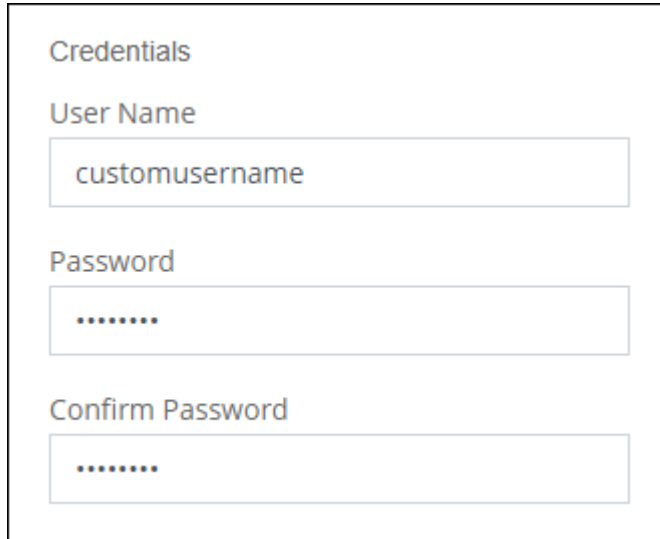
Charging method now displayed

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.



Credentials

User Name

customusername

Password

.....

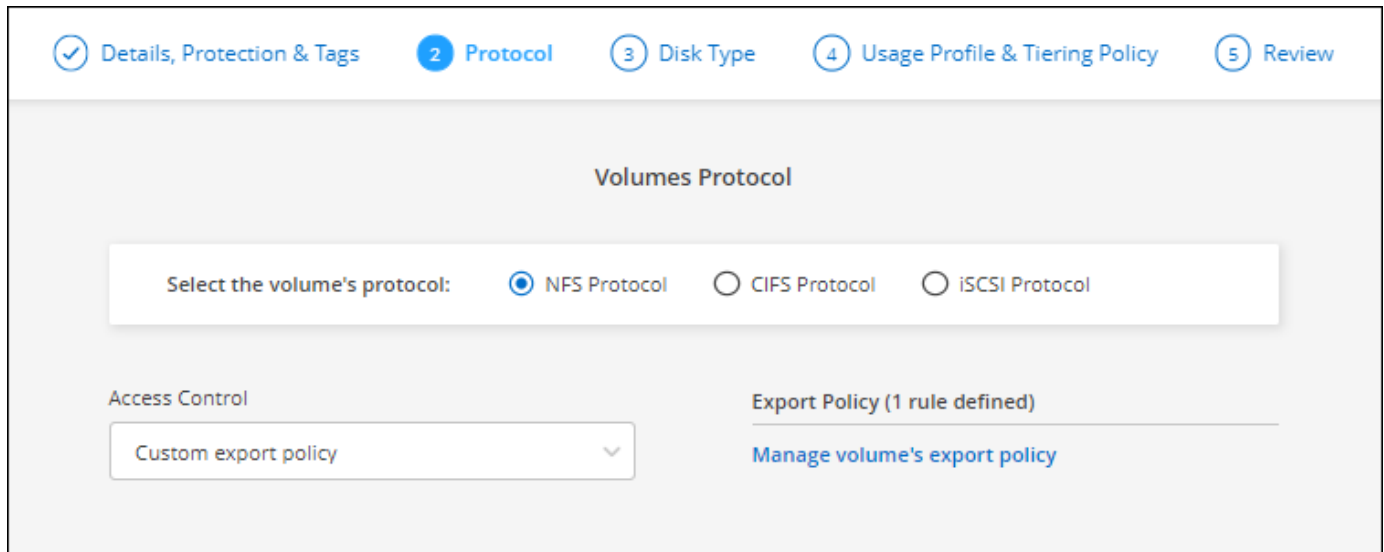
Confirm Password

.....

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.



✓ Details, Protection & Tags 2 Protocol 3 Disk Type 4 Usage Profile & Tiering Policy 5 Review

Volumes Protocol

Select the volume's protocol: ☒ NFS Protocol ☐ CIFS Protocol ☐ iSCSI Protocol

Access Control

Custom export policy

Export Policy (1 rule defined)

[Manage volume's export policy](#)

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.

4 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.

2 September 2021

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

Customer-managed encryption key in Azure

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

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

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

[Learn more about these steps.](#)

7 July 2021

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

New charging methods

New charging methods are available for Cloud Volumes ONTAP.


- **Capacity-based BYOL:** A capacity-based license enables you to pay for Cloud Volumes ONTAP per TiB of capacity. The license is associated with your NetApp account and enables you to create as multiple Cloud Volumes ONTAP systems, as long as enough capacity is available through your license. Capacity-based licensing is available in the form of a package, either *Essentials* or *Professional*.
- **Freemium offering:** Freemium enables you to use all Cloud Volumes ONTAP features free of charge from NetApp (cloud provider charges still apply). You're limited to 500 GiB of provisioned capacity per system and there's no support contract. You can have up to 10 Freemium systems.


[Learn more about these licensing options.](#)

Here's an example of the charging methods that you can choose from:

Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)

☐ Pay-As-You-Go by the hour


☒ Bring your own license

Bring your own license type

Capacity-Based

Package

Professional

☐ Freemium (Up to 500GB)

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](#).

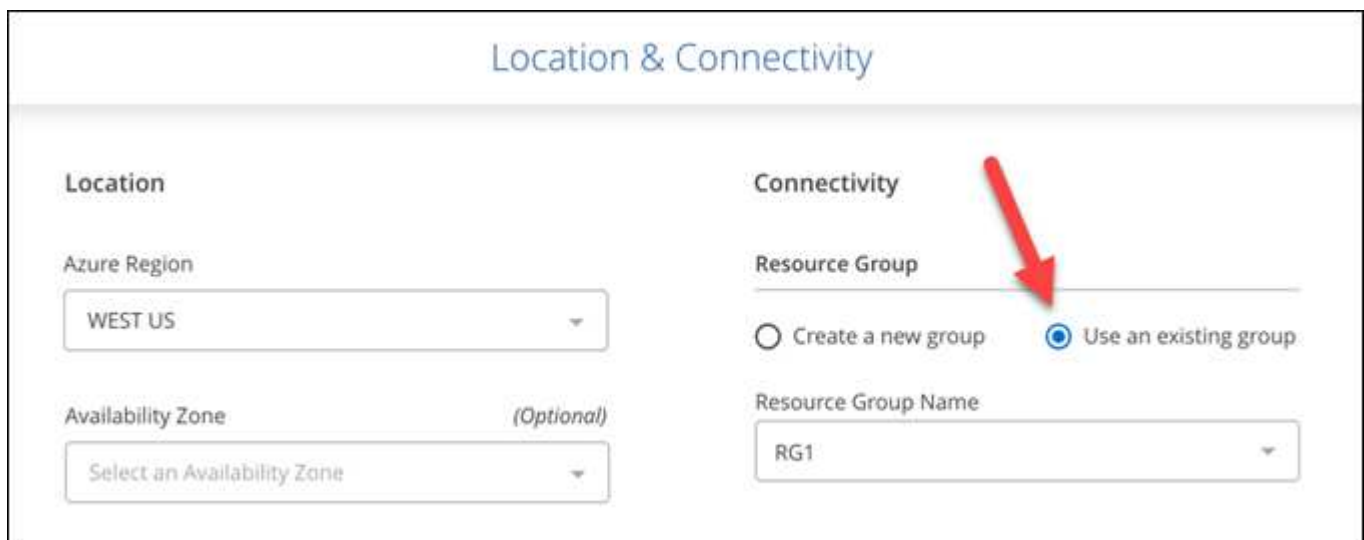
Support for m5dn.24xlarge in AWS

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 GCP.](#)

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.

[Learn more about using gp3 disks with Cloud Volumes ONTAP.](#)

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.

8 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.

[Learn how to get started in C2S.](#)

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.](#)

4 Jan 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

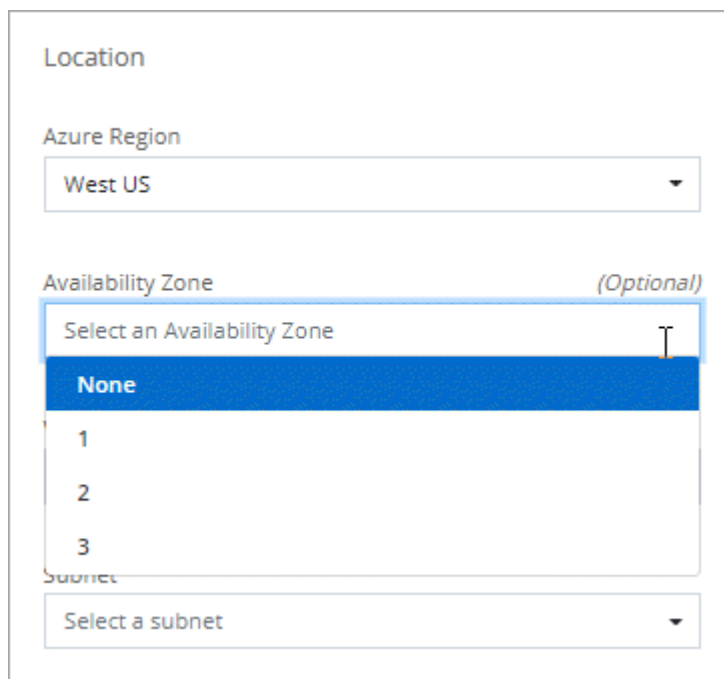
Ultra SSD VNVRAM in supported Azure regions

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.



The screenshot shows a portion of a web-based deployment wizard. At the top, under the heading "Location", there is a dropdown menu for "Azure Region" with "West US" selected. Below this, there is a section for "Availability Zone" with the label "(Optional)". A dropdown menu is open, showing the text "Select an Availability Zone" at the top, followed by a blue bar labeled "None", and then three numbered options: "1", "2", and "3". Below the availability zone section, there is a dropdown menu for "Subnet" with "Select a subnet" selected.

Larger disks in Google Cloud

Cloud Volumes ONTAP now supports 64 TB disks in GCP.



The maximum system capacity with disks alone remains at 256 TB due to GCP 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

3 Nov 2020

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

Azure Private Link for Cloud Volumes ONTAP

By default, 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 BlueXP. To view limitations with the Cloud Volumes ONTAP software itself, [go to the Cloud Volumes ONTAP Release Notes](#)

BlueXP doesn't support FlexGroup volumes creation

While Cloud Volumes ONTAP supports FlexGroup volumes, BlueXP 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 BlueXP's Capacity Management mode to Manual. Automatic mode might not work properly with FlexGroup volumes.



The ability to create FlexGroup volumes in BlueXP is planned for a future release.

BlueXP doesn't support S3 with Cloud Volumes ONTAP

While Cloud Volumes ONTAP supports S3 as an option for scale-out storage, BlueXP doesn't provide any management capabilities for this feature. Using the CLI is the best practice to configure S3 client access from Cloud Volumes ONTAP. For details, refer to the [S3 Configuration Power Guide](#).

[Learn more about Cloud Volumes ONTAP support for S3 and other client protocols.](#)

BlueXP doesn't support disaster recovery for storage VMs

BlueXP 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 BlueXP backup and recovery to deliver backup and restore capabilities for protection, and long-term archive of your cloud data.

[Learn more about BlueXP 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 BlueXP classification helps you understand data context and identify sensitive data.

[Learn more about BlueXP classification](#)



Licenses for ONTAP features are included with Cloud Volumes ONTAP.

[View supported Cloud Volumes ONTAP configurations](#)

Supported ONTAP versions for Cloud Volumes ONTAP deployments

BlueXP enables you to choose from several different ONTAP versions when you create a new Cloud Volumes ONTAP working environment.

Cloud Volumes ONTAP versions other than those listed here are not available for new deployments. For information on upgrade, refer to [Supported upgrade paths](#).

Azure

Single node

- 9.17.1 RC1
- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6

HA pair

- 9.17.1 RC1
- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA

- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

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 BlueXP 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 BlueXP Connector or meet other security and onboarding criteria required for deploying Cloud Volumes ONTAP through BlueXP. 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 BlueXP. After discovery, you can manage them as working environments and take advantage of all the BlueXP capabilities. Refer to [Discover the deployed systems in BlueXP](#).

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 BlueXP.

	Azure marketplace	BlueXP
Onboarding	Shorter and easier, minimal preparation required for direct deployment	Longer onboarding process, including the installation of the BlueXP Connector
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
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

	Azure marketplace	BlueXP
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 BlueXP, 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](#)
- BlueXP deployment: [Quick start for Cloud Volumes ONTAP in Azure](#)
- [BlueXP documentation](#)

Get started in BlueXP

Quick start for Cloud Volumes ONTAP in Azure

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

1

Create a Connector

If you don't have a [Connector](#) yet, you need to create one. [Learn how to create a Connector 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 Connector and access the BlueXP user interface that's running on that Connector. [Learn how to manually install the Connector in a location without internet access](#)

2

Plan your configuration

BlueXP 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

- Ensure that your VNet and subnets will support connectivity between the Connector 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.](#)



Launch Cloud Volumes ONTAP using BlueXP

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

Related links

- [Creating a Connector from BlueXP](#)
- [Creating a Connector from the Azure Marketplace](#)
- [Installing the Connector software on a Linux host](#)
- [What BlueXP 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. BlueXP 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, BlueXP also purchases cloud storage for Cloud Volumes ONTAP system data (boot data, root data, core data, and NVRAM). For planning purposes, it might help for you to review these details before you deploy Cloud Volumes ONTAP.

[View the default disks for Cloud Volumes ONTAP system data in Azure.](#)



The Connector also requires a system disk. [View details about the Connector's default configuration.](#)

Collect networking information

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

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

Choose a write speed

BlueXP 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 BlueXP, 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

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

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 BlueXP Connector also contacts several endpoints for day-to-day operations, as well as the BlueXP web-based console. For information about the BlueXP endpoints, refer to [View endpoints contacted from the Connector](#) and [Prepare networking for using the BlueXP console](#).

Cloud Volumes ONTAP endpoints

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

Endpoints	Applicable for	Purpose	BlueXP deployment modes	Impact if unavailable
https://netapp-cloud-account.auth0.com	Authentication	Used for BlueXP authentication.	Standard and restricted modes.	User authentication fails and the following services remain unavailable: <ul style="list-style-type: none">• Cloud Volumes ONTAP services• ONTAP services• Protocols and proxy services
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://cloudmanager.cloud.netapp.com/tenancy	Tenancy	Used to retrieve the Cloud Volumes ONTAP resources from BlueXP tenancy to authorize resources and users.	Standard and restricted modes.	Cloud Volumes ONTAP resources and the users are not authorized.

Endpoints	Applicable for	Purpose	BlueXP deployment modes	Impact if unavailable
https://support.netapp.com/ods/asupmessage https://support.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://blob.core.windows.net 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 BlueXP operations 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 BlueXP operations 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 BlueXP operations 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 BlueXP operations in Azure.
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 BlueXP operations in Azure.

Network configurations to support Connector proxy

You can use the proxy servers configured for the BlueXP Connector to enable outbound internet access from Cloud Volumes ONTAP. BlueXP 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 Connector proxy configuration. The Connector 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 working environment 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 Connector proxy. When setting up a transparent proxy, the Connector 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 working environment using the [ONTAP CLI: security certificate install](#) command.

For information about configuring proxy servers for the BlueXP Connector, refer to the [Configure a Connector to use a proxy server](#).

IP addresses

BlueXP 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 that BlueXP 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. 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

BlueXP 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

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

Note that BlueXP 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, BlueXP 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—BlueXP manages the Azure Private Link for you. But if you use Azure Private DNS, then you'll need to edit a configuration file. You should also be aware of a requirement for the Connector location in Azure.

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

[Learn more about using Azure Private Links or service endpoints with Cloud Volumes ONTAP.](#)

Connections to other ONTAP systems

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

For instructions, refer to [Microsoft Azure Documentation: Create a Site-to-Site connection in the Azure portal.](#)

Port for the HA interconnect

A Cloud Volumes ONTAP HA pair includes an HA interconnect, which allows each node to continually check

whether its partner is functioning and to mirror log data for the other's nonvolatile memory. The HA interconnect uses TCP port 10006 for communication.

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

Only one HA pair in an Azure resource group

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

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

Security group rules

BlueXP creates Azure security groups that include the inbound and outbound rules for Cloud Volumes ONTAP to operate successfully. [View security group rules for the Connector](#).

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

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

Priority and name	Port and protocol	Source and destination	Description
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 Connector 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
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

Priority and name	Port and protocol	Source and destination	Description
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 create a working environment and choose a predefined security group, you can choose to allow traffic within one of the following:

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



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 Connector 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

Priority and name	Port and protocol	Source and destination	Description
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	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

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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



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

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

Service	Port	Protocol	Source	Destination	Purpose
AutoSupport	HTTPS	443	Node management LIF	support.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	support.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Connector	Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available
Configuration backups	HTTP	80	Node management LIF	http://<connector-IP-address>/occm/offboxconfig	Send configuration backups to the Connector. 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 Connector

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

- [View networking requirements for the Connector](#)
- [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 BlueXP, use the API to create a Cloud Volumes ONTAP working environment that uses the key.

How data is encrypted

BlueXP 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 working environment 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	<ul style="list-style-type: none"> • Boot • Core • NVRAM 	<ul style="list-style-type: none"> • Root • Data
Azure HA single availability zone with page blobs	<ul style="list-style-type: none"> • Boot • Core • NVRAM 	None
Azure HA single availability zone with shared managed disks	<ul style="list-style-type: none"> • Boot • Core • NVRAM 	<ul style="list-style-type: none"> • Root • Data

Cloud Volumes ONTAP configuration	System disks used for key encryption	Data disks used for key encryption
Azure HA multiple availability zones with shared managed disks	<ul style="list-style-type: none"> • Boot • Core • NVRAM 	<ul style="list-style-type: none"> • 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 BlueXP will first create the storage accounts with Microsoft-managed key encryption and then will update 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 working environment. 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 Connector subscription.
 - **Resource group:** Use an existing resource group or create a new one.
 - **Region:** Optionally, select the same region as the Connector.
 - **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 working environment that uses the encryption key

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

Required permissions

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

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

Freemium

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

Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
 - 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](#).

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials
Managed Service Identity

Azure Subscription
OCCM Dev (Default)

Marketplace Subscription
ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

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

Select Charging Method

<input type="radio"/> Professional	By capacity	▼
<input type="radio"/> Essential	By capacity	▼
<input checked="" type="radio"/> Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/> Per Node	By node	▼

[View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.](#)

Capacity-based license

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

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

- A license (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 BlueXP](#)

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

Your license must be available from the BlueXP digital wallet before you can use it with Cloud Volumes ONTAP. If needed, you can [manually add the license to the BlueXP digital wallet](#).

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

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

Select Charging Method

<input checked="" type="radio"/> Professional	By capacity	▼
<input type="radio"/> Essential	By capacity	▼
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/> Per Node	By node	▼

[View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.](#)

PAYGO subscription

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

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

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

Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
 - 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 screenshot shows a dialog box titled "Edit Credentials & Add Subscription". It has a section "Associate Subscription to Credentials" with a help icon. Below this are two dropdown menus: "Credentials" set to "Managed Service Identity" and "Azure Subscription" set to "OCCM Dev (Default)". A message box states: "A marketplace subscription isn't associated with the selected Azure subscription." Below the message is a "+ Add Subscription" link. At the bottom are "Apply" and "Cancel" buttons.

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

The screenshot shows a dialog box titled "Select Charging Method". It lists four options with radio buttons: "Professional", "Essential", "Freemium (Up to 500 GiB)", and "Per Node". To the right of each option is a button labeled "By capacity" (for the first three) or "By node" (for the last one), followed by a dropdown arrow. The "Professional" option is selected.

[View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.](#)



You can manage the Azure Marketplace subscriptions associated with your Azure accounts from the Settings > Credentials page. [Learn how to manage your Azure accounts and subscriptions](#)

Annual contract

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

Steps

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

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

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

2. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
 - 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 BlueXP, select a capacity-based package when you reach the charging methods page.

Select Charging Method

<input checked="" type="radio"/> Professional	By capacity
<input type="radio"/> Essential	By capacity
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity
<input type="radio"/> Per Node	By node

[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 BlueXP 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 Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
 - a. Select the Keystone Subscription charging method when prompted to choose a charging method.

Select Charging Method

☒ **Keystone**

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

☐ Professional

By capacity

☐ Essential

By capacity

☐ Freemium (Up to 500 GiB)

By capacity

☐ Per Node

By node

[View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.](#)

Enable high-availability mode in Azure

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

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

Note the following:

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

result from unplanned failover events.

- Enabling this feature is non-disruptive to Cloud Volumes ONTAP HA pairs.
- Enabling this feature on your Azure subscription 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, BlueXP scans the system every 12 hours to update the internal Azure Load Balancer rules.

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

Steps

1. [Access the Azure Cloud Shell from the Azure Portal](#)
2. Register the high-availability mode feature:

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

3. Optionally verify that the feature is now registered:

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

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

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

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 [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/
  </D>/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 working environment in BlueXP.

Before you begin

You need the following to create a working environment.

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

You should have chose a configuration and obtained Azure networking information from your administrator. For 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 BlueXP 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 BlueXP 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 working environment in BlueXP.

Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the prompts.
3. **Choose a Location:** Select **Microsoft Azure** and **Cloud Volumes ONTAP Single Node**.
4. If you're prompted, [create a Connector](#).
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
Working Environment Name	BlueXP uses the working environment name to name both the Cloud Volumes ONTAP system and the Azure virtual machine. It also uses the name as the prefix for the predefined security group, if you select that option.
Resource Group Tags	<p>Tags are metadata for your Azure resources. When you enter tags in this field, BlueXP adds them to the resource group associated with the Cloud Volumes ONTAP system.</p> <p>You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment.</p> <p>For information about tags, refer to the Microsoft Azure Documentation: Using tags to organize your Azure resources.</p>

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 <i>admin</i> user name or change it to a custom user name.
Edit Credentials	You can choose different Azure credentials and a different Azure subscription to use with this Cloud Volumes ONTAP system. You need to associate an Azure Marketplace subscription with the selected Azure subscription in order to deploy a pay-as-you-go Cloud Volumes ONTAP system. Learn how to add credentials.

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

[Subscribe to BlueXP from the Azure Marketplace](#)

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 BlueXP classification](#)
- [Learn more about BlueXP backup and recovery](#)



If you would like to utilize WORM and data tiering, you must disable BlueXP backup and recovery and deploy a Cloud Volumes ONTAP working environment 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 Connector 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. 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	<p>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.</p> <div>  <p>If the Azure account that you're using has the required permissions, BlueXP removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.</p> </div>
Generated security group	<p>If you let BlueXP generate the security group for you, you need to choose how you'll allow traffic:</p> <ul style="list-style-type: none"> • If you choose Selected VNet only, the source for inbound traffic is the subnet range of the selected VNet and the subnet range of the VNet where the Connector resides. This is the recommended option. • If you choose All VNets, the source for inbound traffic is the 0.0.0.0/0 IP range.
Use existing	<p>If you choose an existing security group, then it must meet Cloud Volumes ONTAP requirements. View the default security group.</p>

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 9.13.1 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.

12. **Subscribe from the Azure Marketplace:** You see this page if BlueXP 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 BlueXP 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:**

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

[Learn more about write speed](#).

- 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](#).

- 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, BlueXP 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)	<p>iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.</p> <p>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.</p> <p>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 bus adapters (HBAs) and are identified by iSCSI qualified names (IQNs).</p> <p>When you create an iSCSI volume, BlueXP 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.</p>

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

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

default

Default Policy

Protocol

NFS
CIFS
iSCSI

Share name: Permissions:

Full Control

Users / Groups:

Valid users and groups separated by a semicolon

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

Field	Description
DNS Primary and Secondary IP Address	<p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p>

Field	Description
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	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <p>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.</p> <p>Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</p>
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	<p>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 BlueXP automation docs for details.</p> <p>Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.</p>

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.

- Review details about the configuration.
- Click **More information** to review details about support and the Azure resources that BlueXP will purchase.
- Select the **I understand...** check boxes.
- Click **Go**.

Result

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

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

For additional help, go to [NetApp Cloud Volumes ONTAP Support](#).

After you finish

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

- If you want to apply quotas to volumes, use 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 working environment in BlueXP.

Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the prompts.
3. If you're prompted, [create a Connector](#).
4. **Details and Credentials:** Optionally change the Azure credentials and subscription, specify a cluster name, add tags if needed, and then specify credentials.

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

Field	Description
Working Environment Name	BlueXP uses the working environment name to name both the Cloud Volumes ONTAP system and the Azure virtual machine. It also uses the name as the prefix for the predefined security group, if you select that option.
Resource Group Tags	<p>Tags are metadata for your Azure resources. When you enter tags in this field, BlueXP adds them to the resource group associated with the Cloud Volumes ONTAP system.</p> <p>You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment.</p> <p>For information about tags, refer to the Microsoft Azure Documentation: Using tags to organize your Azure resources.</p>
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 <i>admin</i> user name or change it to a custom user name.
Edit Credentials	You can choose different Azure credentials and a different Azure subscription to use with this Cloud Volumes ONTAP system. You need to associate an Azure Marketplace subscription with the selected Azure subscription in order to deploy a pay-as-you-go Cloud Volumes ONTAP system. Learn how to add credentials .

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

[Subscribe to BlueXP from the Azure Marketplace](#)

5. **Services:** Enable or disable the individual services based on whether you want to use them with Cloud Volumes ONTAP.
 - [Learn more about BlueXP classification](#)

- [Learn more about BlueXP backup and recovery](#)



If you would like to utilize WORM and data tiering, you must disable BlueXP backup and recovery and deploy a Cloud Volumes ONTAP working environment 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	<p>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.</p> <p>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. BlueXP experiences connection issues if you try to deploy a second Cloud Volumes ONTAP HA pair in an Azure resource group.</p> <div>  <p>If the Azure account that you're using has the required permissions, BlueXP removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.</p> </div>
Generated security group	<p>If you let BlueXP generate the security group for you, you need to choose how you'll allow traffic:</p> <ul style="list-style-type: none"> • If you choose Selected VNet only, the source for inbound traffic is the subnet range of the selected VNet and the subnet range of the VNet where the Connector resides. This is the recommended option. • If you choose All VNets, the source for inbound traffic is the 0.0.0.0/0 IP range.

Field	Description
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 BlueXP updates the system to that version when creating the working environment. 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 BlueXP 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 BlueXP 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 working environment.

[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, BlueXP 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.

Field	Description
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.
Initiator group and IQN (for iSCSI only)	<p>iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.</p> <p>Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.</p> <p>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 bus adapters (HBAs) and are identified by iSCSI qualified names (IQNs).</p> <p>When you create an iSCSI volume, BlueXP 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.</p>

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

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

default

Default Policy

Protocol

NFS
CIFS
iSCSI

Share name: Permissions:

Full Control

Users / Groups:

Valid users and groups separated by a semicolon

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

Field	Description
DNS Primary and Secondary IP Address	<p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p>
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.

Field	Description
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <p>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.</p> <p>Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</p>
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	<p>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 BlueXP automation docs for details.</p> <p>Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.</p>

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.
- Review details about the configuration.
 - Click **More information** to review details about support and the Azure resources that BlueXP will purchase.
 - Select the **I understand...** check boxes.
 - Click **Go**.

Result

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

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

For additional help, go to [NetApp Cloud Volumes ONTAP Support](#).

After you finish

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

Verify Azure platform image

Azure marketplace image verification for Cloud Volumes ONTAP

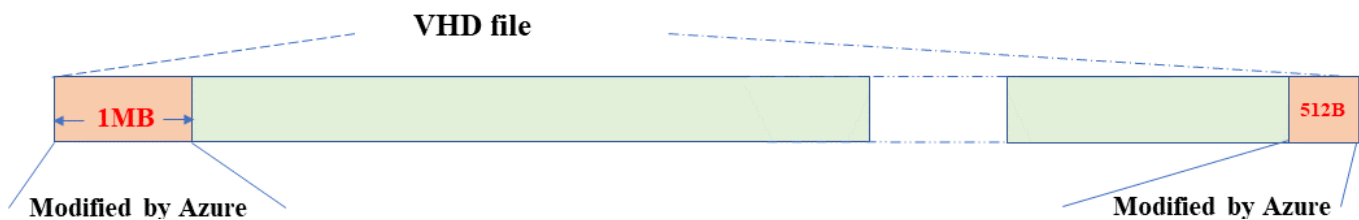
Azure image verification complies with enhanced NetApp security requirements. Verifying an image file is a straightforward process. However, the Azure image signature verification requires specific considerations for the Azure VHD image file because it is altered in the Azure marketplace.



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.

Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

Cloud Volumes ONTAP

Non-Restricted Countries

If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

DOWNLOAD 9150P1_V_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

[View and download checksums](#)

DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]

[View and download checksums](#)

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 [Azure 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	BlueXP	ontap_cloud_gen2
9.16.1	The Azure marketplace	ontap_cloud_direct

9.16.1	BlueXP	ontap_cloud
9.15.1	BlueXP	ontap_cloud
9.15.0	BlueXP, single node deployments	ontap_cloud_byol
9.15.0	BlueXP, 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.blob.core.windows.net/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.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

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="xxxxxxxxxxx"
% 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": "\"0xxxxxxxxxxxxxxxxxxxx\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "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-xxxxxxxx",
    "incrementalCopy": null,
    "progress": "10737418752/10737418752",
    "source": "https://md-
xxxxxx.blob.core.windows.net/xxxxxx/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.blob.core.windows.net/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
```

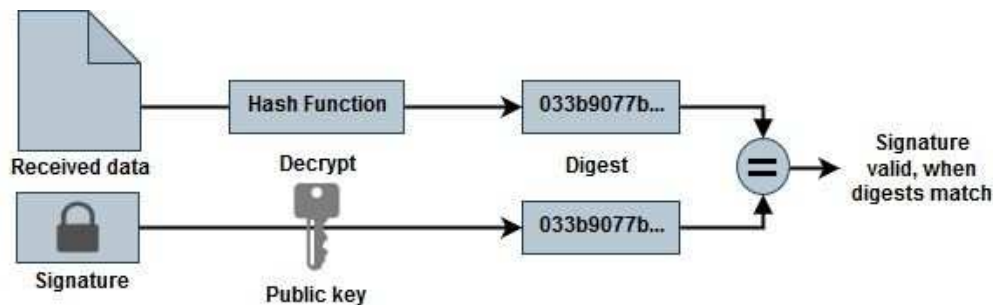
Verify file signature

Azure marketplace image signature verification 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 on BlueXP 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 BlueXP.

- 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 [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 BlueXP

You can discover the Cloud Volumes ONTAP systems that you deployed using Azure marketplace direct

deployment and manage them as working environments in BlueXP. The BlueXP Connector discovers the systems, adds them as working environments, applies the necessary BlueXP licenses, and unlocks the full capabilities of BlueXP 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 BlueXP Connector 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 BlueXP, 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 BlueXP 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 BlueXP Connector can discover the systems only when the deployment is complete and are available for discovery.

Steps

In BlueXP, you follow the standard procedure for discovering existing systems. Refer to [Add an existing Cloud Volumes ONTAP system to BlueXP](#).

After you finish

After the discovery is complete, you can view the systems listed as working environments in BlueXP. 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](#)

Use Cloud Volumes ONTAP

License management

Manage capacity-based licensing for Cloud Volumes ONTAP

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

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

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



While the actual usage and metering for the products and services managed in BlueXP 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 the BlueXP digital wallet

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

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

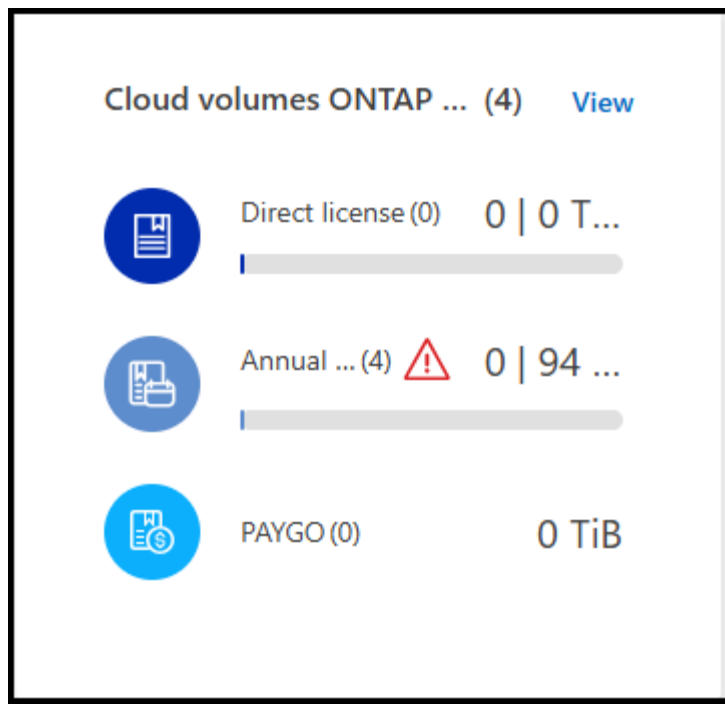
If BlueXP can't add the license, you'll need to manually add them to the digital wallet yourself. For example, if the Connector is installed in a location that doesn't have internet access, you'll need to add the licenses yourself. [Learn how to add purchased licenses to your account.](#)

View the consumed capacity in your account

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

Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
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 BlueXP digital wallet.


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 as follows:
 - Expand a row to view more details.

Provider	Name	Type	Service	Start Date	Status	
	AWS subscription	PAYGO	NetApp BlueXP	Apr 04, 2024	Subscribed	...
NetApp BlueXP			N/A		N/A	
Product Title			Term		Auto Renew	

- 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 BlueXP navigation menu, select **Governance > Digital wallet**.
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**.


Overview > Cloud Volumes ONTAP


Cloud Volumes ONTAP


View

Capacity Based Licenses

[Usage report](#)
[Switch to advanced view](#)


Direct license (0)
0 | 0 TiB


Annual contract (1)
0 | 8 TiB


PAYGO (0)
0 TiB

5. View the details of the package you want to see.

Overview > Cloud Volumes ONTAP


Cloud Volumes ONTAP


View


Capacity Based Licenses

[Switch to standard view](#)

Cloud Volumes ONTAP Packages Summary
[Usage report](#)


0 TiB
Total consumed capacity


8 TiB
Total precommitted capacity


0 TiB
Total PAYGO

Change charging methods

Capacity-based licensing is available in the form of a *package*. When you create a Cloud Volumes ONTAP working environment, you can choose from several licensing packages based on your business needs. If your needs change after you create the working environment, you can change the package at any time. For example, you might change from the Essentials package to the Professional package.

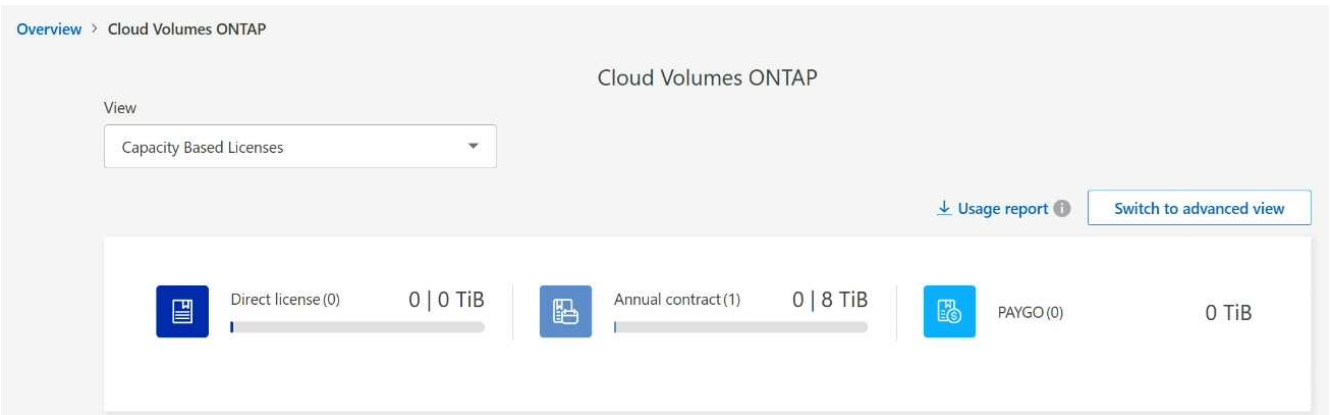
[Learn more about capacity-based licensing packages.](#)

About this task

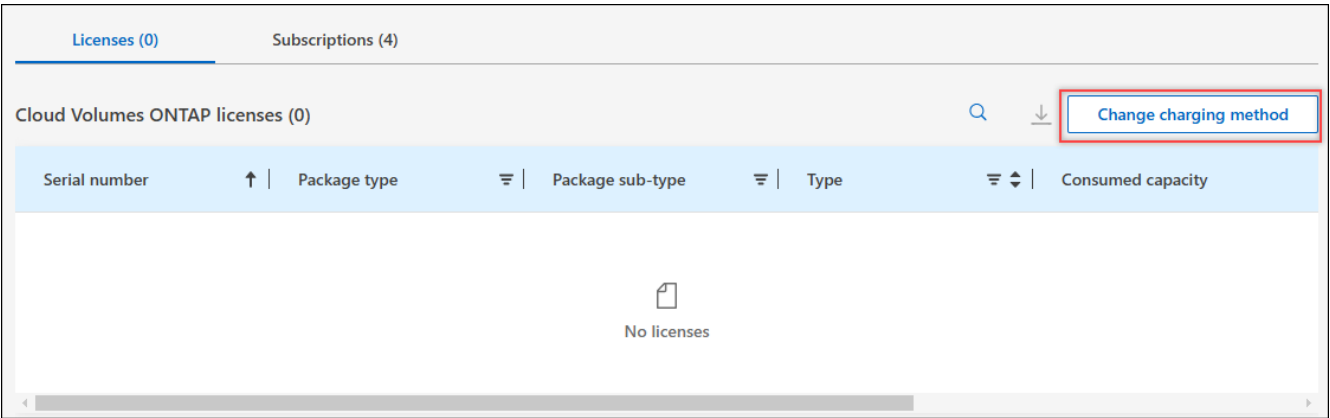
- Changing the charging method doesn't affect whether you're charged through a license purchased from NetApp (BYOL) or from your cloud provider's marketplace pay-as-you-go (PAYGO) subscription.
- BlueXP always attempts to charge against a license first. If a license isn't available, it charges against a marketplace subscription. No "conversion" is required for BYOL 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 BlueXP navigation menu, select **Governance > Digital wallet**.
2. Select the **Overview** tab.
3. On the Cloud Volumes ONTAP tile, select **View**.
4. Select **Switch to advanced view**.



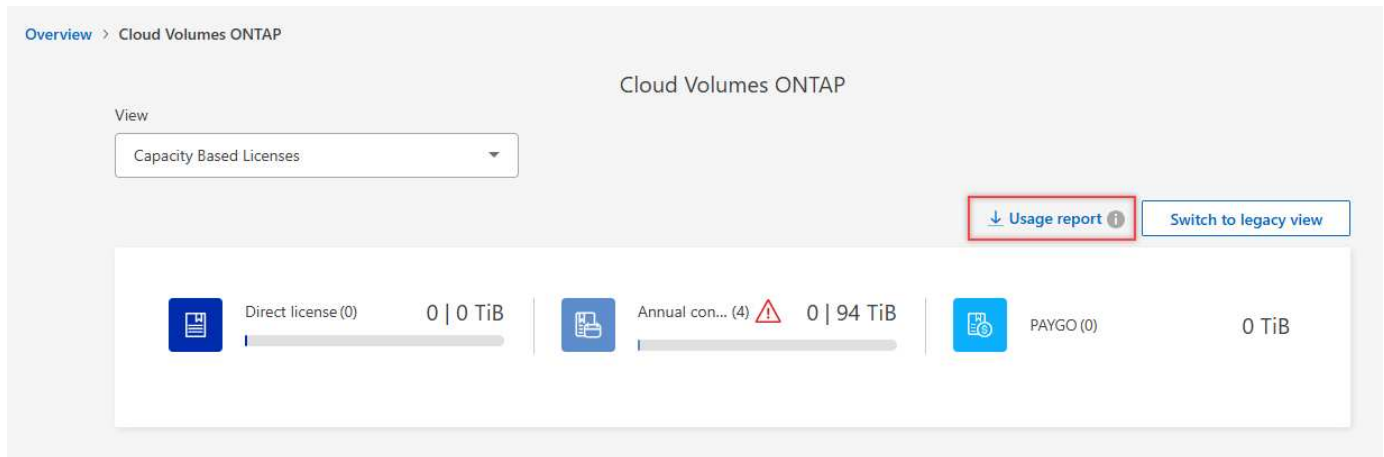
5. Scroll down to the **Capacity-based license** table and select **Change charging method**.



6. On the **Change charging method** pop-up, select a working environment, 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 BlueXP digital wallet. 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:
 - Working environment ID and name (appears as the UUID)
 - Cloud
 - NetApp account ID
 - Working environment 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 working environment. This information is not available on any screen in the digital wallet. It includes the following information:
 - Working environment 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 BlueXP navigation menu, select **Governance > Digital wallet**.
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 through BlueXP

Manage your Keystone subscriptions from the BlueXP digital wallet 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 on-premises ONTAP clusters or 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 BlueXP, you need to contact NetApp to authorize

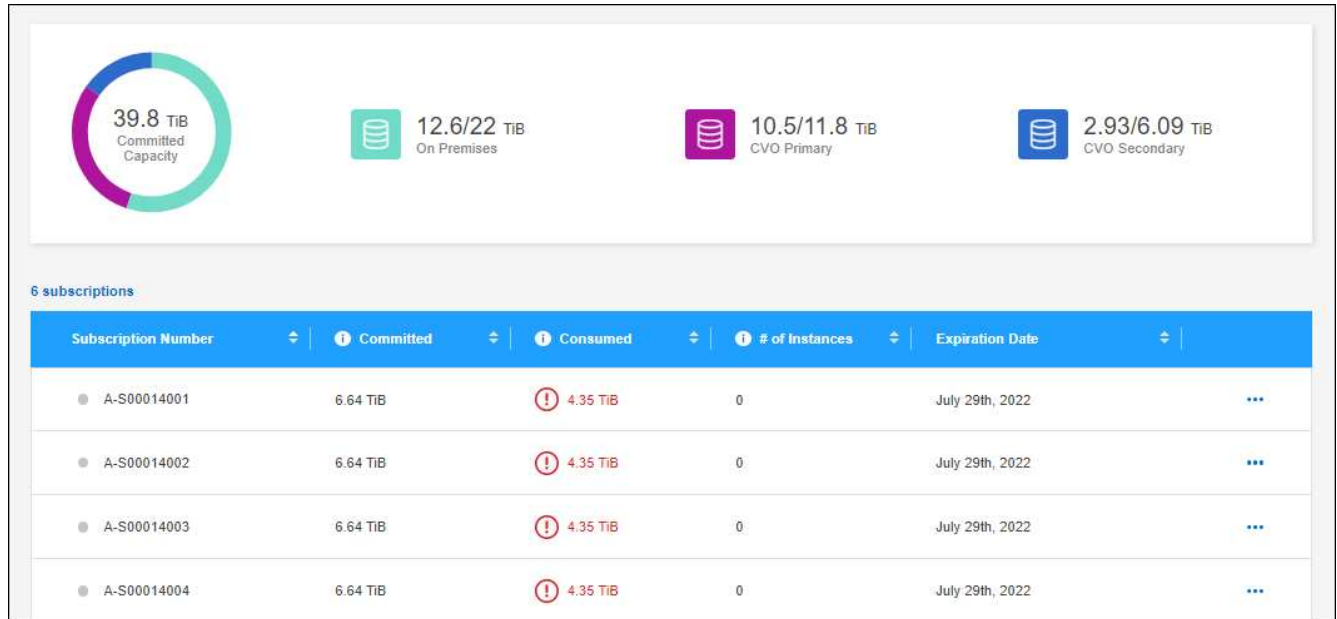
your BlueXP user account with your Keystone subscriptions.

Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
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 user account to access the subscriptions.

4. Come back to the **Keystone Subscriptions** tab to view your subscriptions.



The screenshot displays the Keystone Subscriptions interface. At the top, there are four capacity usage cards: a donut chart for '39.8 TiB Committed Capacity', a green card for '12.6/22 TiB On Premises', a purple card for '10.5/11.8 TiB CVO Primary', and a blue card for '2.93/6.09 TiB CVO Secondary'. Below these, a section titled '6 subscriptions' contains a table with the following data:

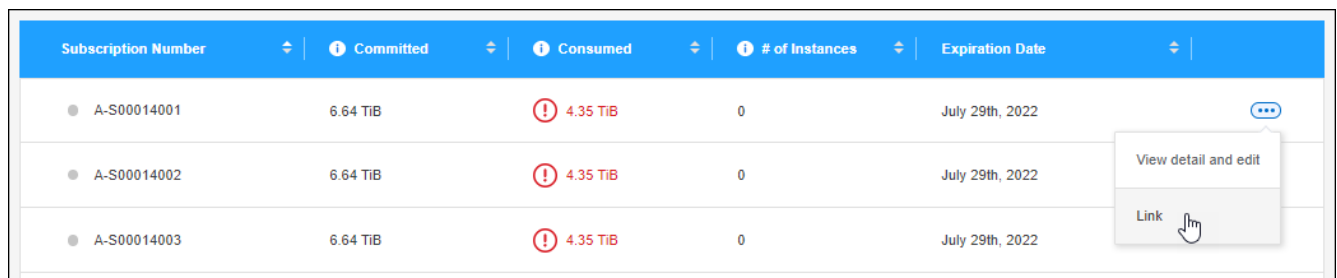
Subscription Number	Committed	Consumed	# of Instances	Expiration Date
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022
A-S00014004	6.64 TiB	4.35 TiB	0	July 29th, 2022

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 BlueXP navigation menu, select **Governance > Digital wallet**.
2. Select **Keystone Subscriptions**.
3. For the subscription that you want to link, click **...** and select **Link**.



This screenshot shows the same subscription table as the previous image, but with a context menu open for the first row (A-S00014001). The menu includes the option 'Link', which is highlighted by a mouse cursor.

Subscription Number	Committed	Consumed	# of Instances	Expiration Date
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022

Result

The subscription is now linked to your BlueXP 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 BlueXP. Requesting additional capacity for a service level provides more storage for on-premises clusters or for Cloud Volumes ONTAP systems.

Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
2. Select **Keystone Subscriptions**.
3. For the subscription that you want adjust the capacity, click **...** and select **View detail and edit**.
4. Enter the requested committed capacity for one or more subscriptions.

Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity
Extreme	0.977 TiB	0.293 TiB	<input type="text" value="Enter amount"/> TiB
Premium	0.977 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB
Performance	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
Standard	0.732 TiB	0.439 TiB	<input type="text" value="Enter amount"/> TiB
Value	0.977 TiB	 0.879 TiB	<input type="text" value="Enter amount"/> TiB
Data Tiering	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
CVO Primary	1.96 TiB	 1.76 TiB	<input type="text" value="3"/> TiB
CVO Secondary	1.02 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB

Additional Information

Is there anything else we should know about your request?
Please be as descriptive as possible.

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 BlueXP digital advisor dashboard enables you to monitor Keystone subscription usage and to generate reports.

[Learn more about monitoring subscription usage](#)

Unlink a subscription

If you no longer want to use a Keystone subscription with BlueXP, 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 BlueXP navigation menu, select **Governance > Digital wallet**.
2. Select **Keystone**.
3. For the subscription that you want to unlink, click **...** and select **Unlink**.

Result

The subscription is unlinked from your BlueXP 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 BlueXP digital wallet to ensure that each Cloud Volumes ONTAP system has a valid license with the required capacity.

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

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

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

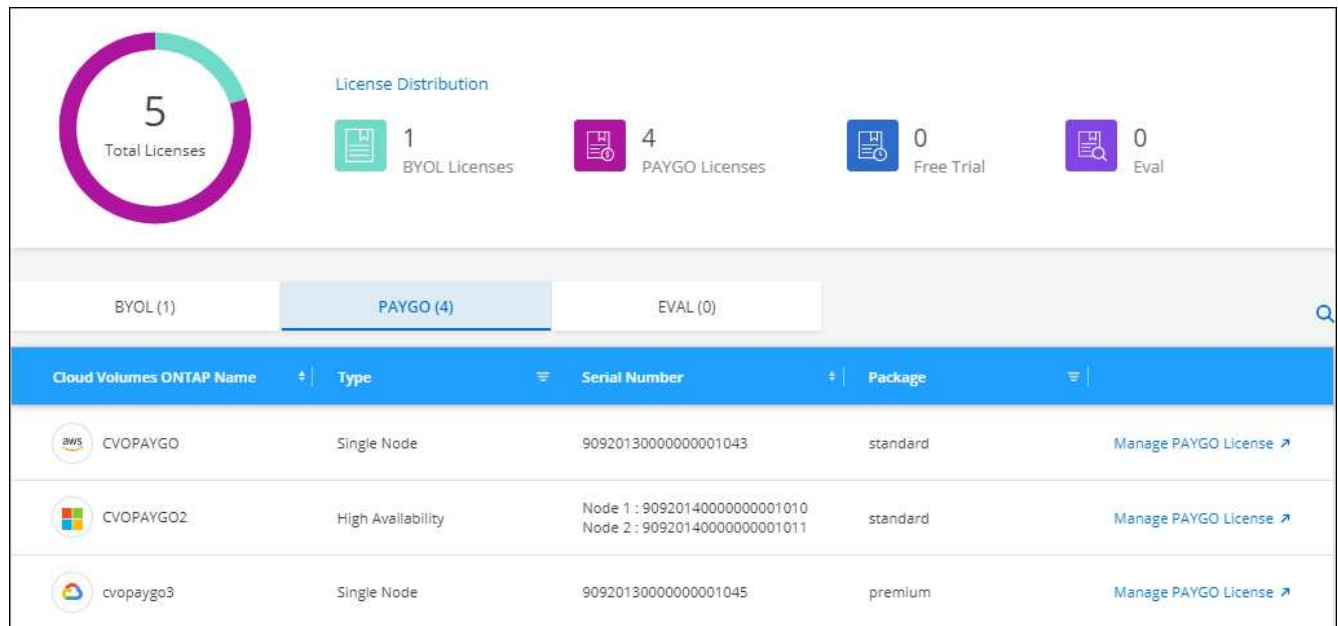
[Learn more about Cloud Volumes ONTAP licenses.](#)

Manage PAYGO licenses

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

Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
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 BlueXP digital wallet so that you can select the license when you create a new Cloud Volumes ONTAP system. The digital wallet identifies these licenses as *unassigned*.

Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
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

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

Exchange unassigned node-based licenses

If you have an unassigned node-based license for Cloud Volumes ONTAP that you haven't used, you can exchange the license by converting it to a BlueXP backup and recovery license, a BlueXP classification license, or a BlueXP 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 BlueXP navigation menu, select **Governance > Digital wallet**.
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**.

BYOL (14)	Eval (2)	Unassigned (3)	PAYGO (6)		Q	Add Unassigned Licenses
Serial Number	Type	Cloud Provider	License Expiry	Status		
012345678901234567890	Single Node	All Providers	April 20, 2022	Unassigned	Exchange License	...
012345678901234567891	Single Node	 Azure	April 20, 2022	Unassigned	Exchange License	...
012345678901234567892	Single Node	 AWS	January 1, 2022	Exchanged to Cloud Tiering on August 1, 2021		...

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

BlueXP 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, BlueXP 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

License Generator

The following fields are pre-populated based on the NetApp SSO login provided.
To download the corresponding NetApp license file, re-enter your SSO password along with the correct Product Line and Product Serial number.

First Name: Ben

Last Name:

Company: Network Appliance, Inc

Email Address:

Username:

Product Line*

Not only is protecting your data required by law, it's also the right thing to do.

☐ I have read NetApp's new Global Data Privacy Policy and I agree to the terms and conditions.

ONTAP Select - Standard

ONTAP Select - Premium

ONTAP Select - Premium XL

Cloud Volumes ONTAP for AWS (single node)

Cloud Volumes ONTAP for AWS (HA)

Cloud Volumes ONTAP for GCP (single node or HA)

Cloud Volumes ONTAP for Microsoft Azure (single node)

Cloud Volumes ONTAP for Microsoft Azure (HA)

Service Level Manager - SLO Advanced

StorageGRID Webscale

StorageGRID WhiteBox

SnapCenter Standard (capacity-based)

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, BlueXP automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system. If BlueXP can't access the license file over the secure internet connection, you can obtain the file yourself and then manually upload the file to BlueXP.

Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
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

BlueXP 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 BlueXP. After you purchase the license, you can apply it to a Cloud Volumes ONTAP system.

Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
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 BlueXP.

Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
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 BlueXP navigation menu, select **Governance > Digital wallet**.

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

[Learn how to replicate data between systems](#)

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

[Learn how to delete a Cloud Volumes ONTAP working environment.](#)

Related links

<https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/azure/concept-licensing.html#end-of-availability-of-node-based-licenses> End of availability of node-based licenses
[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 BlueXP.

BlueXP provides several ways to create a new volume:

- Specify details for a new volume and let BlueXP 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, BlueXP 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.

Create a volume

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

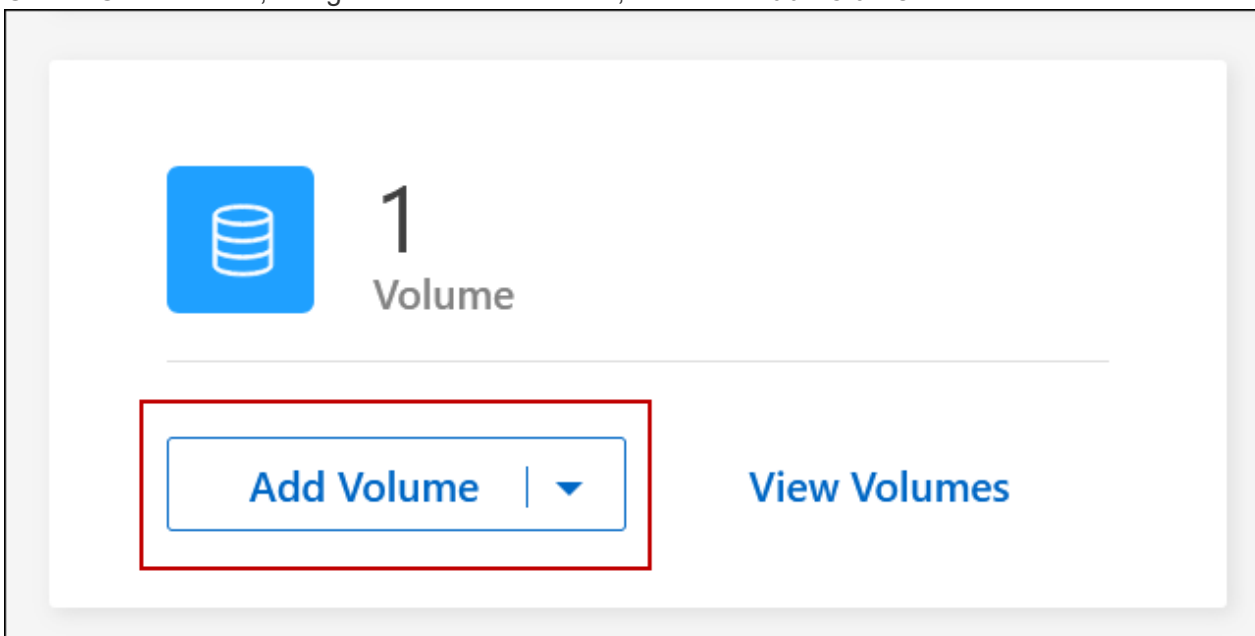
Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, double-click the name of the Cloud Volumes ONTAP system on which you want to provision a FlexVol volume.
3. Create a new volume by letting BlueXP 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.

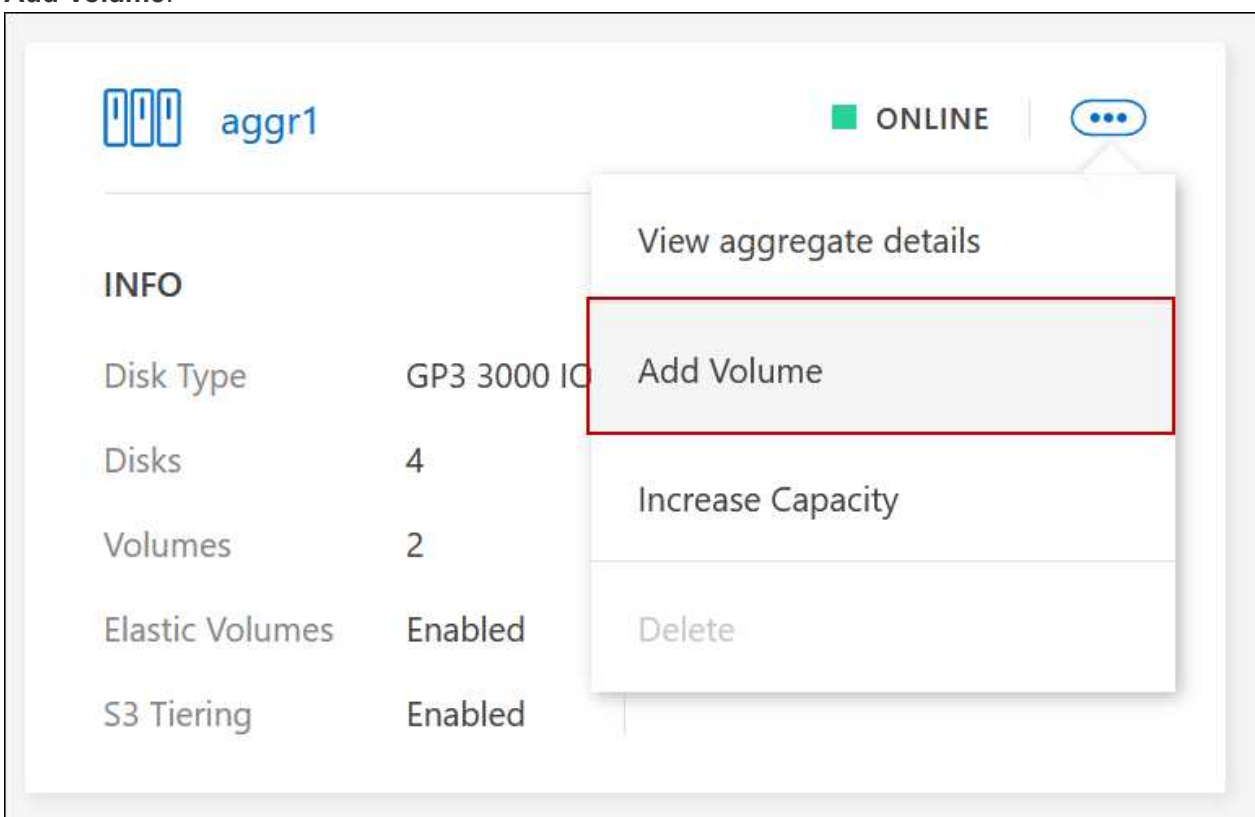
Any aggregate

On the Overview tab, navigate to the Volumes tile, and click **Add Volume**.



Specific aggregate

On the Aggregates tab, navigate to the desired aggregate tile. Click the menu icon, and then click **Add Volume**.



4. 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.
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, BlueXP 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, BlueXP enters a value that provides access to all instances in the subnet.

CIFS

Permissions and users/groups

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

DNS Primary and Secondary IP Address

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

Active Directory Domain to join

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

Credentials authorized to join the domain

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

CIFS server NetBIOS name

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

Organizational Unit

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

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

DNS Domain

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

NTP Server

Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. For information, refer to the [BlueXP 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, BlueXP 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 bus adapters (HBAs) and are identified by iSCSI qualified names (IQNs).

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

- [Sizing your system in Azure](#)

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

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

Thin provisioning

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

Deduplication

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

Compression

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

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

Result

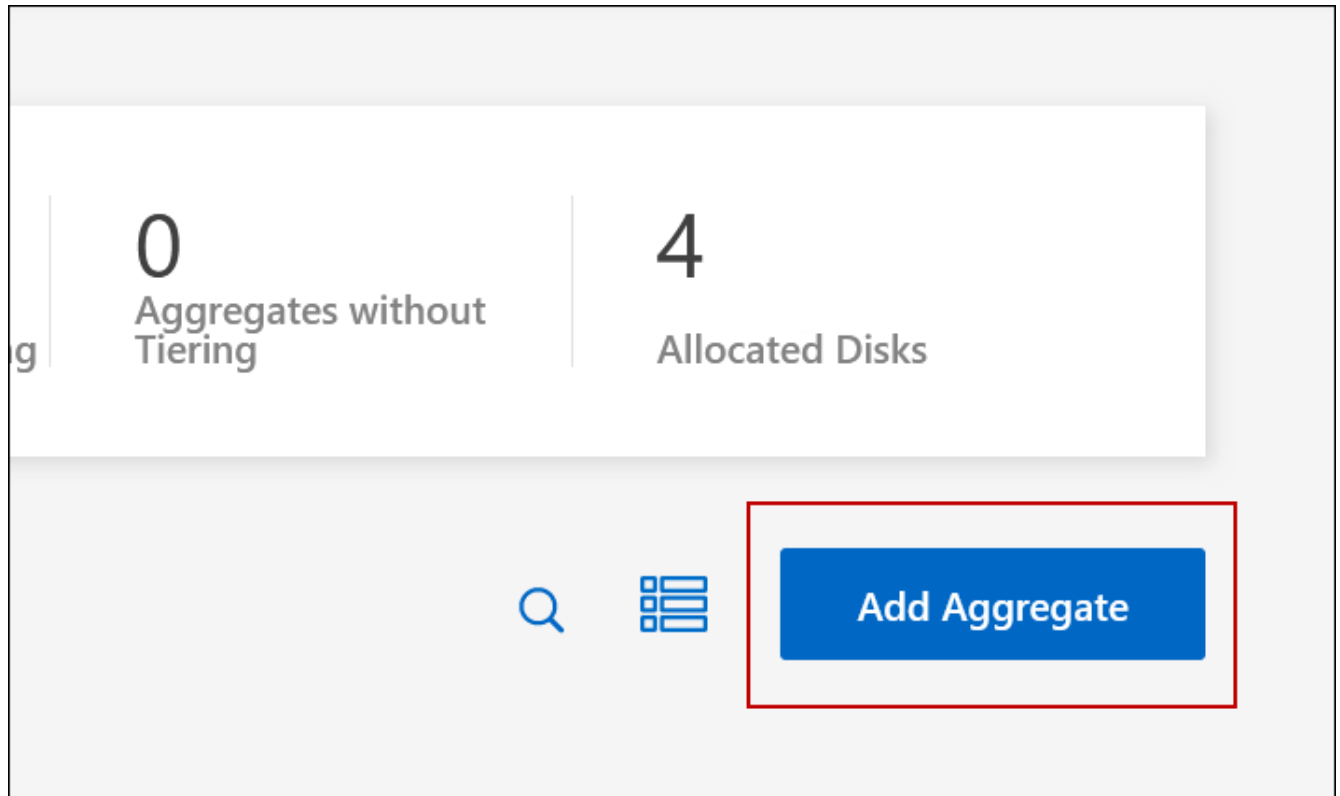
BlueXP creates the volume on the Cloud Volumes ONTAP system.

Create a volume on the second node in an HA configuration

By default, BlueXP 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 > Canvas**.
2. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
3. On the Aggregates tab, click **Add Aggregate**.
4. From the *Add Aggregate* screen, create the aggregate.



5. For Home Node, choose the second node in the HA pair.
6. After BlueXP creates the aggregate, select it and then click **Create volume**.
7. Enter details for the new volume, and then click **Create**.

Result

BlueXP creates the volume on the second node in the HA pair.

After you create a volume

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

If you want to apply quotas to volumes, you must use 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

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

You can manage volumes in BlueXP Standard View or through ONTAP System Manager that is included within

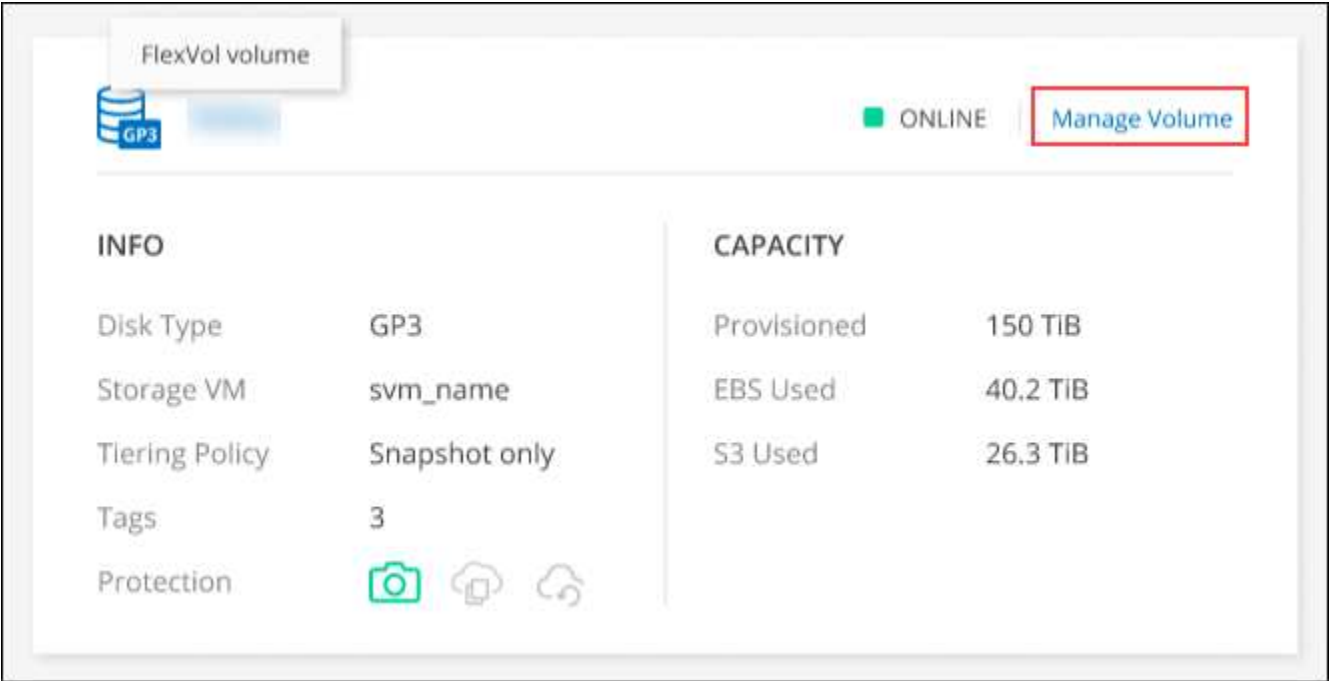
BlueXP for advanced volume management. The Standard View provides a limited set of options to modify your volumes. System Manager provides advanced level of management, such as cloning, resizing, changing settings for anti-ransomware, analytics, protection, and activity tracking, and moving volumes across tiers. For information, refer to [Administer Cloud Volumes ONTAP using System Manager](#).

Manage volumes

By using the Standard View of BlueXP, 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 > Canvas**.
- 2. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.
- 3. In the working environment, click the **Volumes** tab.



- 4. On the Volumes tab, navigate to the desired volume title and then click **Manage volume** to access the Manage Volumes right-side panel.

Task	Action
View information about a volume	Under Volume Actions in the Manage volumes panel, click View volume details .
Get the NFS mount command	<div>a. Under Volume Actions in the Manage volumes panel, click Mount Command.</div> <div>b. Click Copy.</div>

Task	Action
Clone a volume	<ol style="list-style-type: none"> Under Volume Actions in the Manage volumes panel, click Clone the volume. Modify the clone name as needed, and then click Clone. <p>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.</p> <p>To learn more about FlexClone volumes, refer to the ONTAP 9 Logical Storage Management Guide.</p>
Edit a volume (read-write volumes only)	<ol style="list-style-type: none"> Under Volume Actions in the Manage volumes panel, click Edit volume settings Modify the volume's Snapshot policy, NFS protocol version, NFS access control list (export policy), or share permissions, and then click Apply. <div>  <p>If you need custom Snapshot policies, you can create them by using ONTAP System Manager.</p> </div>
Delete a volume	<ol style="list-style-type: none"> Under Volume Actions in the Manage volumes panel, click Delete the volume. Under the Delete Volume window, enter the name of the volume you want to delete. Click Delete again to confirm.
Create a Snapshot copy on demand	<ol style="list-style-type: none"> Under Protection Actions in the Manage Volumes panel, click Create a Snapshot copy. Change the name, if needed, and then click Create.
Restore data from a Snapshot copy to a new volume	<ol style="list-style-type: none"> Under Protection Actions in the Manage Volumes panel, click Restore from Snapshot copy. Select a Snapshot copy, enter a name for the new volume, and then click Restore.
Change the underlying disk type	<ol style="list-style-type: none"> Under Advanced Actions in the Manage Volumes panel, click Change Disk Type. Select the disk type, and then click Change. <div>  <p>BlueXP moves the volume to an existing aggregate that uses the selected disk type or it creates a new aggregate for the volume.</p> </div>


Task	Action
Change the tiering policy	<ol style="list-style-type: none"> Under Advanced Actions in the Manage Volumes panel, click Change Tiering Policy. Select a different policy and click Change. <div>  <p>BlueXP moves the volume to an existing aggregate that uses the selected disk type with tiering, or it creates a new aggregate for the volume.</p> </div>
Delete a volume	<ol style="list-style-type: none"> Select a volume, and then click Delete. Type the name of the volume in the dialog. 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 Connector's settings.

If you need to resize your volume, you can do it from ONTAP System Manager in BlueXP.

Steps

- Click the System Manager view to resize a volume through ONTAP System Manager. Refer to [How to get started](#).
- From the left navigation menu, select **Storage > Volumes**.
- From the list of volumes, identify the one that you should resize.
- Click the options icon .
- Select **Resize**.
- 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.
- Click **Save**.

Resize volume ✕

CAPACITY

25

GiB

SNAPSHOT RESERVE %

1

Existing	New
DATA SPACE	DATA SPACE
20 GiB	24.75 GiB
SNAPSHOT RESERVE	SNAPSHOT RESERVE
0 Bytes	256 MiB

Cancel
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 working environment, 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.
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.

Task	Action
DNS Primary and Secondary IP Address	<p>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</p> <p>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.</p>
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	<p>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</p> <ul style="list-style-type: none"> 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. <p>Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain</p>

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 BlueXP displays an Action Required message

BlueXP 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.



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

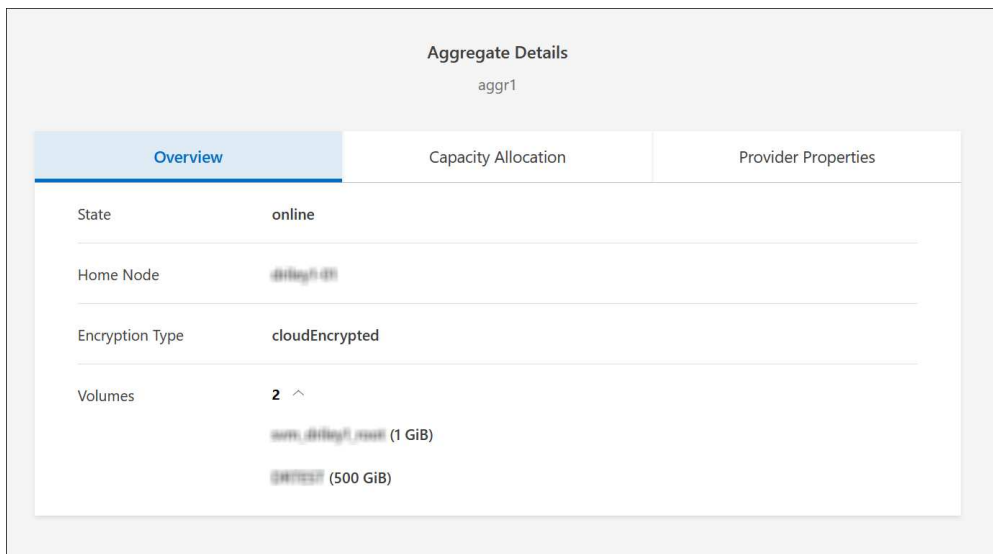
Steps

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

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

2. Identify one or more volumes to move out of the aggregate:
 - a. In the working environment, click the **Aggregates** tab.
 - b. Navigate to the desired aggregate tile, and then click the ... (ellipses icon) > **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, BlueXP cannot perform this action for you because the system has reached the disk limit.

Steps

1. Identify a Cloud Volumes ONTAP system that has available capacity, or deploy a new system.
2. Drag and drop the source working environment on the target working environment to perform a one-time data replication of the volume.

For 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.

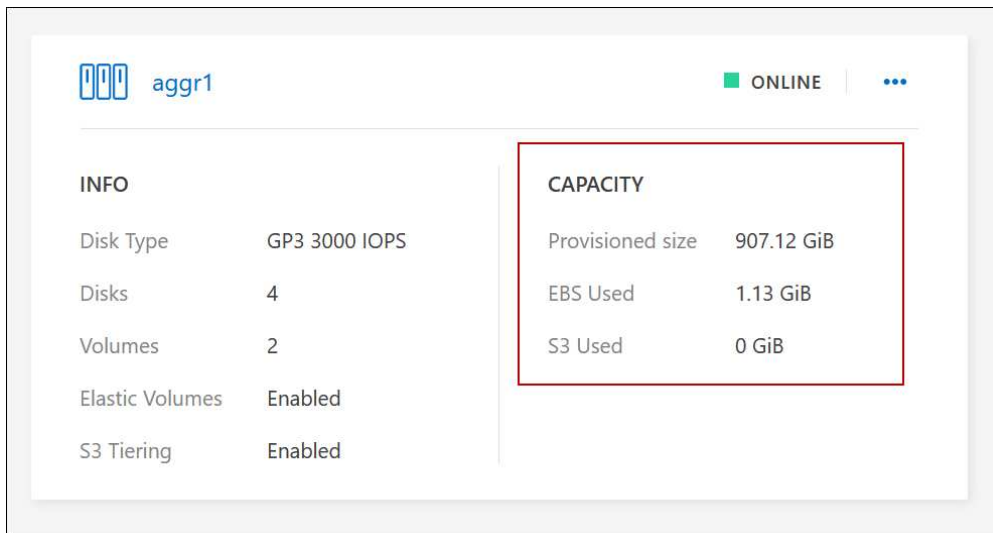
About this task

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, BlueXP cannot perform this action for you.

Steps

1. Verify whether an existing aggregate has available capacity for the volumes that you need to move:
 - a. In the working environment, click the **Aggregates** tab.
 - b. Navigate to the desired aggregate tile, and then click the ... (**ellipses icon**) > **View aggregate details**.
 - c. Under the aggregate tile, 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 ... (**ellipses 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:

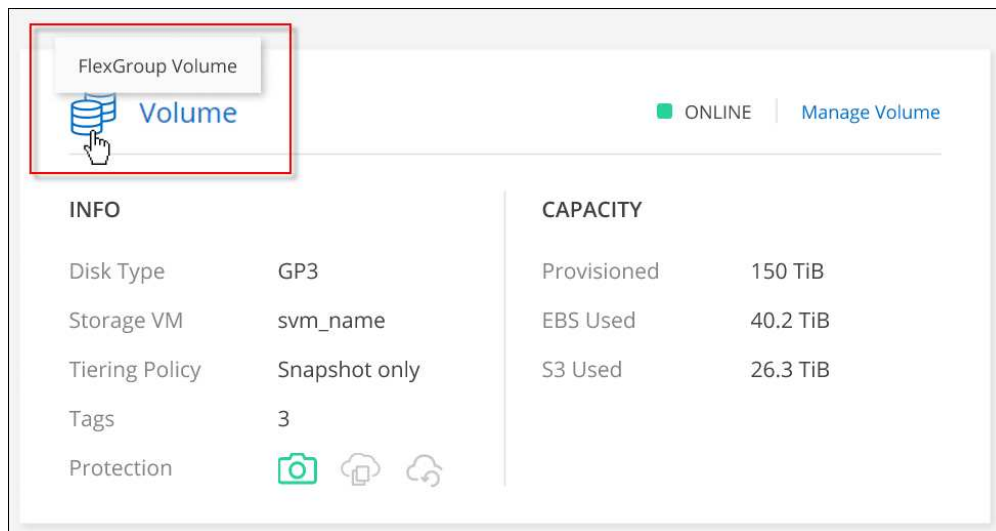
- The volume is a clone.
- The volume is a parent of a clone.
- The source or destination aggregate has a single Throughput Optimized HDD (st1) disk.
- One of the aggregates uses an older naming scheme for objects. Both aggregates have to use the same name format.

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 within BlueXP. Identical to the information provided for FlexVol volumes, BlueXP provides detailed information for created FlexGroup volumes through a dedicated Volumes tile. Under the Volumes tile, 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.



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.

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 Azure, you won't need to do anything as long as BlueXP has the required permissions. [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

BlueXP 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. BlueXP does that for you.
- You don't need to enable data tiering at the system level.



BlueXP 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 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.

Feature interoperability

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

Requirements

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

Requirements to tier cold data to Azure Blob storage

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

Connector has these permissions:

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

The custom role includes the permissions by default. [View Azure permission for the Connector](#)

Enable data tiering after implementing the requirements

BlueXP 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 BlueXP user interface 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**

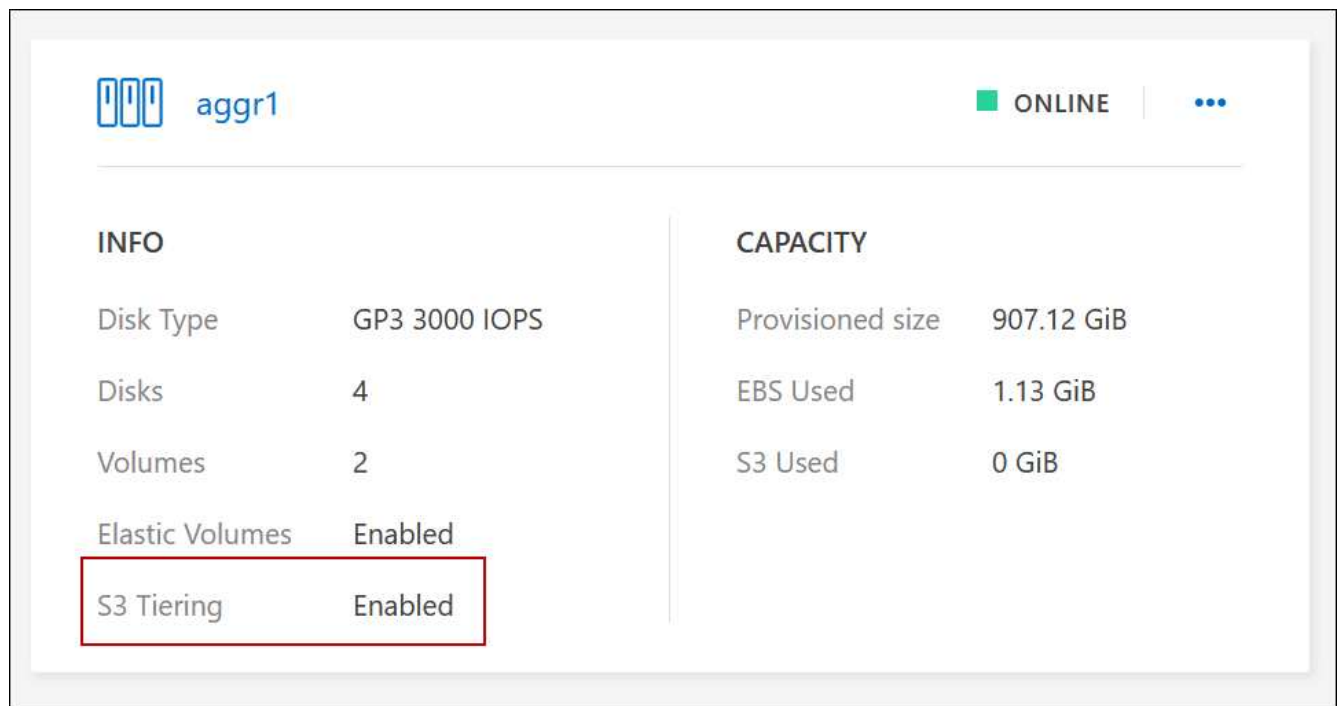
If you're enabling data tiering on a new volume, then you don't need to worry about enabling data tiering on an aggregate. BlueXP creates the volume on an existing aggregate that has tiering enabled, or it creates a new aggregate for the volume if a data tiering-enabled aggregate doesn't already exist.

- **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. Open the working environment in BlueXP.
2. Click the Aggregates tab.
3. Navigate to the desired tile and verify whether 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 Volumes tab under the working environment, create a new volume or change the tier of an existing volume:

Task	Action
Create a new volume	Click Add New Volume .
Modify an existing volume	Select the 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

Change Tiering Policy

Volume_1

Tiering Policy

☒ **Auto** - Tiers cold Snapshot copies and cold user data from the active file system to object storage.
Minimum cooling days: 31 (2-183)


☐ **All** - Immediately tiers all data (not including metadata) to object storage.

☐ **Snapshot Only** - Tiers cold Snapshot copies to object storage.

☐ **None** - Data tiering is disabled.

S3 Storage classes Standard-Infrequent Access

S3 Storage Encryption Key aws/s3

 This action is non-disruptive and changing the tier impacts cost, performance, and maximum capacity. Refer to [BlueXP documentation](#) for more details.

BlueXP 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 > Canvas**.
2. On the Canvas page, select the working environment that contains the source volume, and then drag it to the working environment to which you want to replicate the volume.
3. Follow the prompts until you reach the tiering page and enable data tiering to object storage.

Example

 **S3 Tiering**

 What are storage tiers?

☒ **Enabled** ☐ **Disabled**

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

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. From the working environment, click the menu icon and then click **Storage Classes** or **Blob Storage Tiering**.
2. Choose a storage class and then click **Save**.

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. BlueXP can then purchase additional disks for you when additional capacity is required (up until you reach the disk limit for the aggregate).

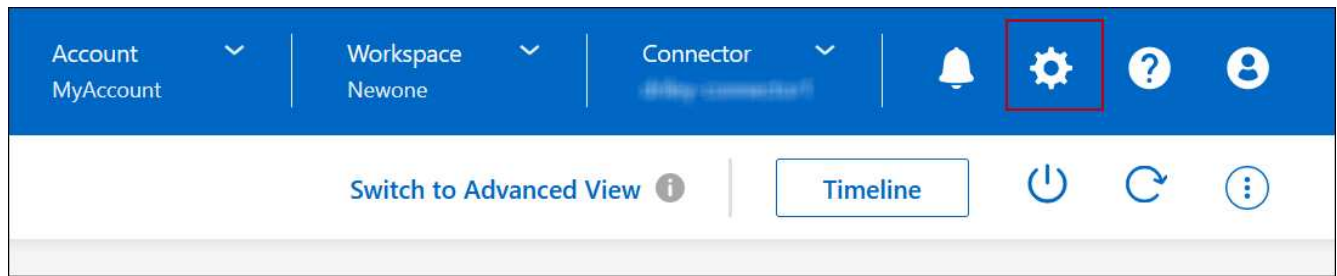


If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data and you might experience performance degradation. Any change should be done with caution. If you're unsure, reach out to NetApp Support for guidance.

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

Steps

1. In the upper right of the BlueXP console, click the **Settings** icon, and select **Cloud Volumes ONTAP Settings**.



2. Under **Capacity**, click **Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering**.
3. Change the free space ratio based on your requirements and click **Save**.

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 working environment

You can delete an S3 bucket with the data tiered from a Cloud Volumes ONTAP working environment when you decommission the environment.

You can delete the S3 bucket only if:

- The Cloud Volume ONTAP working environment is deleted from BlueXP.
- All objects are deleted from the bucket and the S3 bucket is empty.

When you decommission a Cloud Volumes ONTAP working environment, 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: vservers object-store-server bucket delete](#).

Connect to a LUN on Cloud Volumes ONTAP from your host system

When you create an iSCSI volume, BlueXP 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:

- BlueXP's automatic capacity management doesn't apply to LUNs. When BlueXP 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 > Canvas**.
2. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.
3. In the working environment, click the **Volumes** tab.
4. On the Volumes tab, navigate to the desired volume title and then click **Manage volume** to access the Manage Volumes right-side panel.
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.

BlueXP provides management of FlexCache volumes with the [BlueXP volume caching](#) service.

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 Azure, you need to set up Azure Key Vault for NetApp Volume Encryption (NVE). For information, refer to [Manage keys with Azure Key Vault](#).
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](#)

Aggregate administration

Create an aggregate for Cloud Volumes ONTAP systems

You can create aggregates yourself or let BlueXP 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 BlueXP. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, double-click the name of the Cloud Volumes ONTAP instance on which you want to manage aggregates.
3. On the Aggregates tab, click **Add Aggregate** and then specify details for the aggregate.

Azure

For help with disk type and disk size, refer to [Plan your Cloud Volumes ONTAP configuration in Azure](#).

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

Manage aggregates 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 BlueXP. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

Before you begin

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

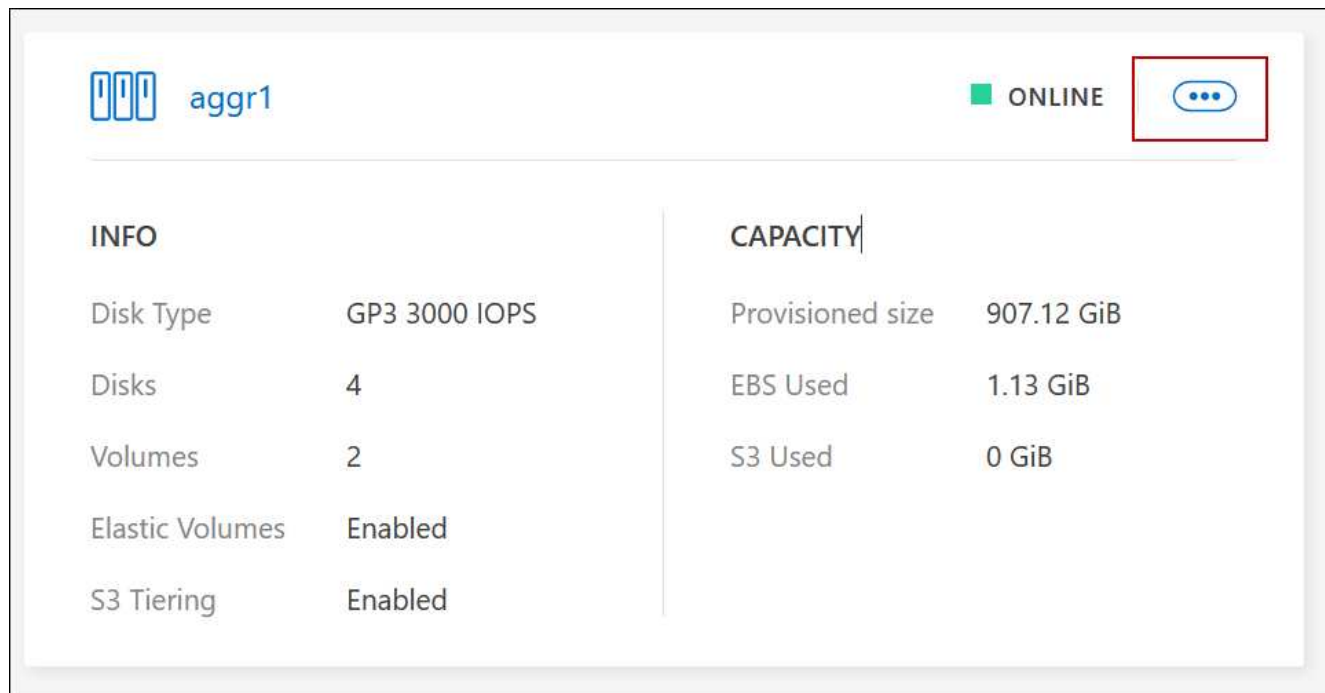
About this task

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 > Canvas**.

2. On the Canvas page, double-click the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
3. In the working environment, click the **Aggregates** tab.
4. On the Aggregates tab, navigate to the desired title and then click the ... (ellipses icon).



5. Manage your aggregates:

Task	Action
View information about an aggregate	Under the ... (ellipses icon) menu, click View aggregate details .
Create a volume on a specific aggregate	Under the ... (ellipses icon) menu, click Add volume .
Add disks to an aggregate	<ol style="list-style-type: none"> Under the ... (ellipses icon) menu, click Add disks. Select the number of disks that you want to add and click Add. <div>  All disks in an aggregate must be the same size. </div>
Delete an aggregate	<ol style="list-style-type: none"> Select an aggregate tile that does not contain any volumes click the ... (ellipses icon) > Delete. Click Delete again to confirm.

Manage the Cloud Volumes ONTAP aggregate capacity on a Connector

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

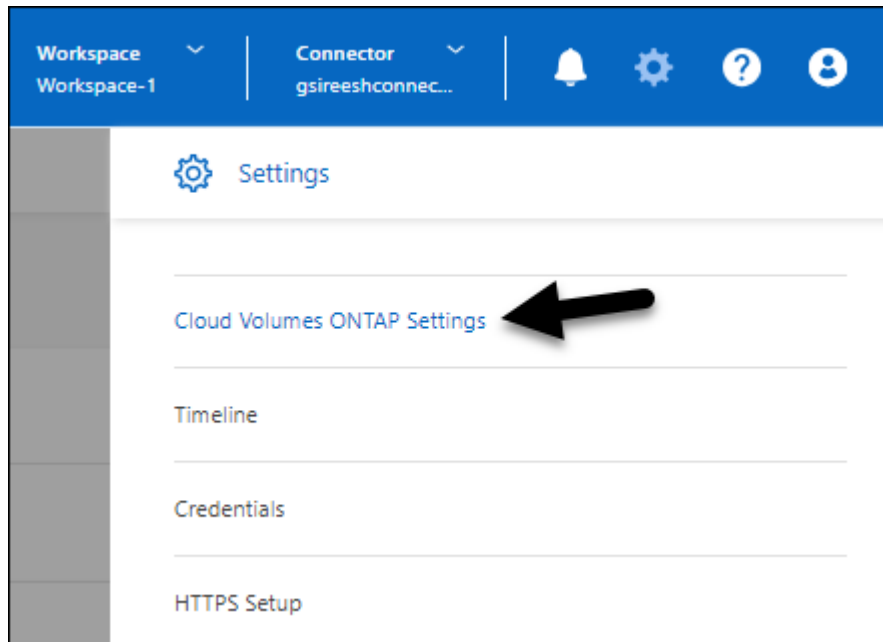
These settings affect all Cloud Volumes ONTAP systems managed by a Connector. If you have another Connector, it can be configured differently.

Required permissions

BlueXP Organization or Account admin privileges are required to modify Cloud Volumes ONTAP Settings.

Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Cloud Volumes ONTAP Settings**.



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

Capacity Management Mode

Choose whether BlueXP notifies you of storage capacity decisions or whether BlueXP automatically manages 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:

$$(\text{aggregate capacity} - \text{total used capacity on the aggregate}) / \text{aggregate capacity}$$

Refer to [Automatic capacity management](#) to learn how 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.

3. Click **Save**.

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

BlueXP 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.

Details & Protection

Storage VM Name

svm_name1

Volume Name

Size (GiB)

Volume size

Snapshot Policy

default

Default Policy

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

Destination Volume Name

volume_copy

Destination Storage VM Name

svm_name1

Destination Aggregate

Automatically select the best aggregate

Modify the name of the default storage VM

BlueXP 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 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 BlueXP 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, BlueXP 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 BlueXP APIs.

About this task

When you create storage VMs using the APIs, along with configuring the required network interfaces, BlueXP 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 Connector 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 BlueXP APIs, you can rename and delete storage VMs in both single node and HA configurations.

Before you begin

The Connector 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 BlueXP REST APIs](#)

Set up storage VM disaster recovery for Cloud Volumes ONTAP

BlueXP 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:

- Azure Key Vault (AKV)

New aggregates will have NAE enabled by default after you set up an external key manager. New volumes that aren't part of an NAE aggregate will have NVE enabled by default (for example, if you have existing aggregates that were created before setting up an external key manager).

Cloud Volumes ONTAP doesn't support onboard key management.

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 BlueXP](#)
- [Register pay-as-you-go systems](#)



BlueXP doesn't install the NVE license on systems that reside in the China region.

Steps

1. Review the list of supported key managers in the [NetApp Interoperability Matrix Tool](#).



Search for the **Key Managers** solution.

2. [Connect to the Cloud Volumes ONTAP CLI.](#)
3. Configure external key management.
 - Azure: [Azure Key Vault \(AKV\)](#)

Manage 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



- 1 Permissions 2 Principal 3 Application (optional) 4 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

- 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.

Create an access policy

Permissions

2 Principal

3 Application (optional)

4 Review + create

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Search by object ID, name, or email address

Selected item
No item selected

Previous

Next

- Click **Next** two times until you arrive at **Review and create**. Then, click **Create**.
- Select **Next** to advance to **Networking** options.
- 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.)
- 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

- In the menu for the Key Vault you have created for Cloud Volumes ONTAP, navigate to the **Keys** option.
- Select **Generate/import** to create a new key.
- Leave the default option set to **Generate**.
- Provide the following information:
 - Encryption key name

- Key type: RSA
- RSA key size: 2048
- Enabled: Yes

5. Select **Create** to create the encryption key.
6. Return to the **Keys** menu and select the key you just created.
7. Select the key ID under **Current version** to view the key properties.
8. Locate the **Key Identifier** field. Copy the URI up to but not including the hexadecimal string.

Create an Azure Active Directory Endpoint (HA only)

1. This process is only required if you are configuring Azure Key Vault for an HA Cloud Volumes ONTAP Working Environment.
2. In the Azure portal navigate to **Virtual Networks**.
3. Select the Virtual Network where you deployed the Cloud Volumes ONTAP working environment and select the **Subnets** menu on the left side of the page.
4. Select the subnet name for you Cloud Volumes ONTAP deployment from the list.
5. Navigate to the **Service Endpoints** heading. In the drop-down menu, select the following:
 - **Microsoft.AzureActiveDirectory**
 - **Microsoft.KeyVault**
 - **Microsoft.Storage** (optional)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

Save

Cancel

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: ekvip_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 documentation: About Azure Key Vault](#)
- [ONTAP command reference guide](#)

Enable NetApp ransomware protection solutions for Cloud Volumes ONTAP









Ransomware attacks can cost a business time, resources, and reputation. BlueXP 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 through BlueXP, the Ransomware Protection setting allows you to utilize the ONTAP FPolicy functionality to guard against common ransomware file extension types.

Steps

1. On the Canvas page, double-click the name of the system you configure to ransomware protection.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Ransomware Protection**.

Information		Features
Working Environment Tags		Tags 
Scheduled Downtime		Off 
S3 Storage Classes	Standard-Infrequent Access 	
Instance Type		m5.xlarge 
Write Speed		Normal 
Ransomware Protection		Off 
Support Registration		Not Registered 
CIFs Setup		

3. Implement the NetApp solution for ransomware:

- 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



BlueXP creates this scope when you activate FPolicy on Cloud Volumes ONTAP. The list is based on common ransomware file types. You can customize the blocked file extensions by using the `vserver fpolicy policy scope` commands from the Cloud Volumes ONTAP CLI.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection

50 % Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

2 Block Ransomware File Extensions

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names

Activate FPolicy

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.

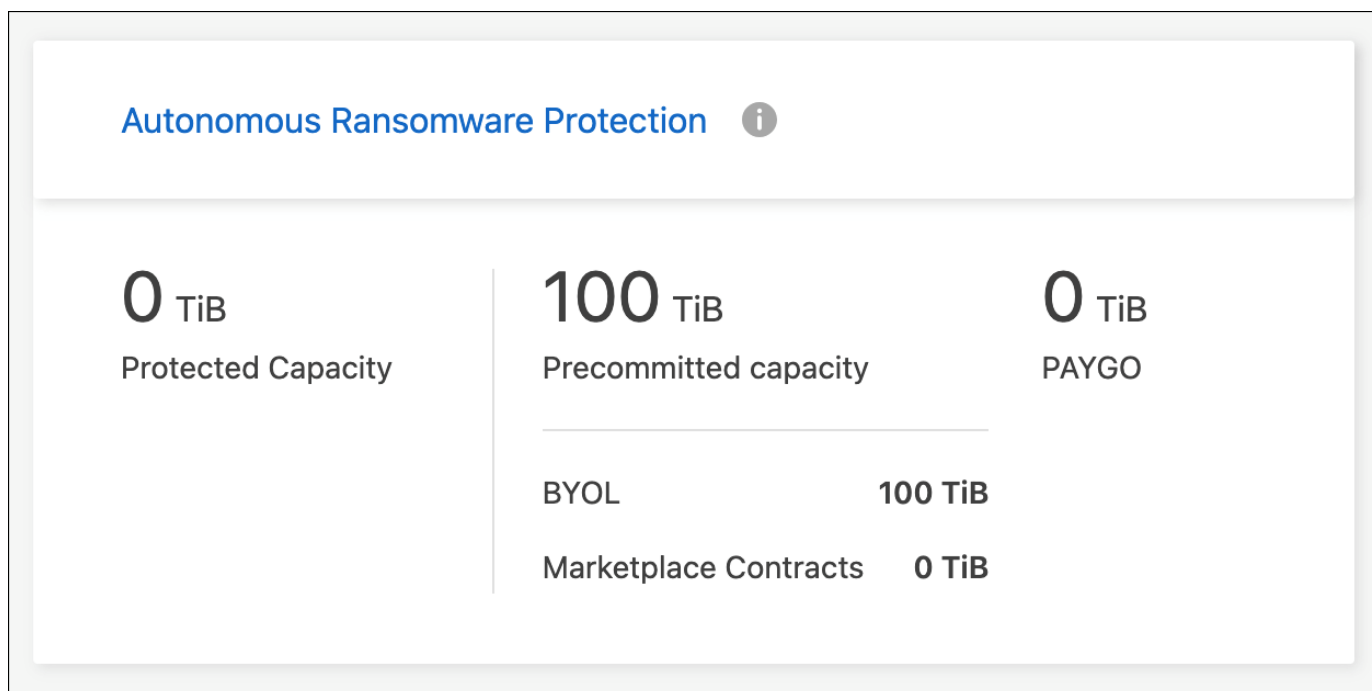
Separate from the file extension protections provided through the [ransomware protection setting](#), the ARP feature uses workload analysis to alert the user on potential attacks based on detected "abnormal activity". Both the ransomware protection setting and the ARP feature can be used in conjunction 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.

System administration

Upgrade Cloud Volumes ONTAP software

Upgrade Cloud Volumes ONTAP from BlueXP 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 BlueXP only

Upgrades of Cloud Volumes ONTAP must be completed from BlueXP. You should not upgrade Cloud Volumes ONTAP by using ONTAP System Manager or the ONTAP CLI. Doing so can impact system stability.

How to upgrade

BlueXP provides two ways to upgrade Cloud Volumes ONTAP:

- By following upgrade notifications that appear in the working environment
- By placing the upgrade image at an HTTPS location and then providing BlueXP with the URL

Supported upgrade paths

The version of Cloud Volumes ONTAP that you can upgrade to depends on the version of Cloud Volumes ONTAP that you're currently running.

Current version	Versions that you can directly upgrade to
9.16.1 (for Azure and Google Cloud only)	9.17.1 (for Azure and Google Cloud only)
9.15.1	9.16.1 (for Azure and Google Cloud only)
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

Current version	Versions that you can directly upgrade to
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

Note the following:

- The supported upgrade paths for Cloud Volumes ONTAP are different than they are for an on-premises ONTAP cluster.
- If you upgrade by following the upgrade notifications that appear in a working environment, BlueXP 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 in BlueXP 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 BlueXP. For example, if the current GA release is 9.13.1, patches for 9.11.1-9.13.1 appear in BlueXP. If you want to upgrade to a patch release for versions 9.11.1 or below, you will need to use the manual upgrade procedure by [downloading the ONTAP image](#).

As a general rule for patch (P) releases, you can upgrade from one version release to any P-release of the current version you're running or the next version.

Here are a couple of examples:

- 9.13.0 > 9.13.1P15
- 9.12.1 > 9.13.1P2

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 BlueXP 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

BlueXP 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 BlueXP 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.

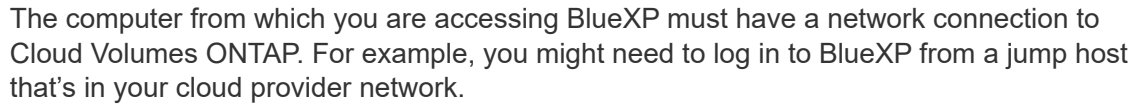
About this task

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 working environment.



- ## Verify that aggregates are online

About this task

Steps

- | Aggregate Details | | |
|---------------------|--------------------|---------------------|
| aggr1 | | |
| Overview | | Capacity Allocation |
| Provider Properties | | |
| State | online | |
| Home Node | http://10.10.10.10 | |
| Encryption Type | cloudEncrypted | |
| Volumes | 2 | |

- ### 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

BlueXP 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 BlueXP notifications](#).

Another way to perform software upgrades by using an image on an external URL. This option is helpful if BlueXP 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 BlueXP notifications

BlueXP 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 BlueXP notification, 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

BlueXP 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 > Canvas**.
2. Select a working environment.

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.

Upgrade Cloud Volumes ONTAP Version



You are about to upgrade Cloud Volumes ONTAP ⓘ

9.12.1 → 9.13.1P10 (Jul 7, 2024)

Select other versions

End User License Agreement (EULA)

1. DEFINITIONS
1.1. "Documentation" means technical documentation describing the features and functions of the Software.
1.2. "NetApp Cloud Provider" means a third party authorized by NetApp to offer or enable the use of the Software as part of such provider's cloud-based service.
1.3. "NetApp Partner" means an authorized NetApp distributor, reseller or other channel partner. 1.4. "Open Source Software" means third party software that is openly and freely licensed under the terms of a public

☐ I read and approve the End User License Agreement (EULA)

Upgrade

Cancel

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**.

Select the ONTAP version you want to upgrade to:

Version	Date
<input type="radio"/> 9.12.1P14	Aug 22, 2024
<input type="radio"/> 9.12.1P13	Jul 7, 2024
<input type="radio"/> 9.13.1P10	Jul 7, 2024
<input type="radio"/> 9.13.1P9	May 9, 2024

☒ All versions

Write the version you want to upgrade to:

Write the version here

Save Cancel

Apply Cancel

6. In the Upgrade Cloud Volumes ONTAP page, read the EULA, and then select **I read and approve the EULA**.
7. Click **Upgrade**.
8. To check the status of the upgrade, click the Settings icon and select **Timeline**.

Result

BlueXP starts the software upgrade. You can perform actions on the working environment 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 Connector or on an HTTP server and then initiate the software upgrade from BlueXP. You might use this option if BlueXP can't access the S3 bucket to upgrade the software.

Before you begin

- BlueXP 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 BlueXP.

Go to the NetApp Knowledge Base to view step-by-step instructions:

[NetApp KB: How to configure BlueXP 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 Connector or on an HTTP server from which the file will be served.

Two paths are available. The correct path depends on your Connector version.

- `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
- `/opt/application/netapp/cloudmanager/ontap/images/`

5. From the working environment in BlueXP, click the ... (**ellipses 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 Connector in the path shown above, you would enter the following URL:

`http://<Connector-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

BlueXP starts the software update. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

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 BlueXP 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 BlueXP, go to **Account Settings** and add it now.

[Learn how to add NetApp Support Site accounts.](#)

2. On the Canvas page, double-click the name of the system you want to register..
3. On the Overview tab, click the Features panel and then click the pencil icon next to **Support Registration**.

Information		Features
Working Environment Tags	Tags	
Scheduled Downtime	Off	
S3 Storage Classes	Standard-Infrequent Access	
Instance Type	m5.xlarge	
Write Speed	Normal	
Ransomware Protection	Off	
Support Registration	Not Registered	
CI Fs Setup		

4. Select a NetApp Support Site account and click **Register**.

Result

BlueXP registers the system 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 BlueXP license conversion tool.

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 BlueXP license conversion tool 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 BlueXP user credentials.
- The working environment 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 the BlueXP account. This license can be a marketplace subscription or a BYOL/private offer package in BlueXP digital wallet.
- 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 Canvas page, double-click the name of the working environment 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 working environment 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 BlueXP digital wallet post conversion. If the conversion is not complete, then even on selecting this checkbox, the license will not be deleted from the digital wallet. If you have a marketplace subscription, this option is unavailable.
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 BlueXP digital wallet.

Pricing in different hyperscalars

For details on pricing, go to the [NetApp BlueXP website](#).

For information about private offers in specific hyperscalars, write to:

- AWS - awsपो@netapp.com
- Azure - azureपो@netapp.com
- Google Cloud - gcpपो@netapp.com

Start and stop a Cloud Volumes ONTAP system

You can stop and start Cloud Volumes ONTAP from BlueXP 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 BlueXP 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, BlueXP postpones the shutdown if an active data transfer is in progress.









BlueXP 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 Canvas page, double-click the desired working environment.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Scheduled Downtime**.

Information		Features
Working Environment Tags	Tags	
Scheduled Downtime	Off	
S3 Storage Classes	Standard-Infrequent Access	
Instance Type	m5.xlarge	
Write Speed	Normal	
Ransomware Protection	Off	
Support Registration	Not Registered	
CI/CD Setup		

3. Specify the shutdown schedule:

- Choose whether you want to shut down the system every day, every weekday, every weekend, or any combination of the three options.
- 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 BlueXP to shut down the system every Saturday at 20:00 P.M. (8:00 PM) for 12 hours. BlueXP restarts the system every Monday at 12:00 a.m.

Schedule Downtime

Cloud Manager Time Zone: 17:58 UTC

Select when to turn off your Working Environment:

Turn off every day

Sun, Mon, Tue, Wed, Thu, Fri, Sat

at

20

 :

00

 for

12

 hours (1-24)

Turn off every weekdays

Mon, Tue, Wed, Thu, Fri

at

20

 :

00

 for

12

 hours (1-24)

Turn off every weekend

Sat

at

20

 :

00

 for

12

 hours (1-48)

4. Click **Save**.

Result

BlueXP saves the schedule. 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.



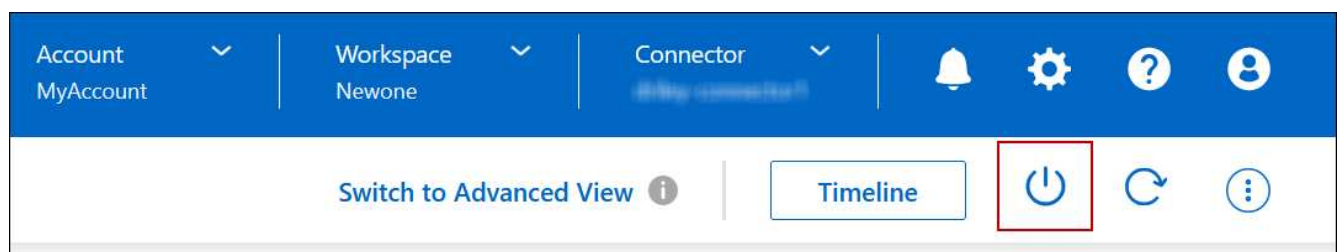
To reduce costs, BlueXP periodically deletes older snapshots of root and boot disks. Only the two most recent snapshots are retained for both the root and boot disks.

About this task

When you stop an HA pair, BlueXP shuts down both nodes.

Steps

1. From the working environment, click the **Turn off** icon.



2. Keep the option to create snapshots enabled because the snapshots can enable system recovery.
3. Click **Turn Off**.

It can take up to a few minutes to stop the system. You can restart systems at a later time from the working environment page.



Snapshots are created automatically upon reboot.

Synchronize Cloud Volumes ONTAP system time using the NTP server

Specifying an NTP server synchronizes the time between the systems in your network, which can help prevent issues due to time differences.

Specify an NTP server using the [BlueXP API](#) or from the user interface when you [create a CIFS server](#).

Modify system write speed

BlueXP enables you to choose a normal or high write speed for Cloud Volumes ONTAP. The default write speed is normal. You can change to high write speed if fast write performance is required for your workload.

High write speed is supported with all types of single node systems and some HA pair configurations. View supported configurations in the [Cloud Volumes ONTAP Release Notes](#)

Before you change the write speed, you should [understand the differences between the normal and high settings](#).

About this task

- Ensure that operations such as volume or aggregate creation are not in progress.
- Be aware that this change restarts the Cloud Volumes ONTAP system. This is disruptive process that requires downtime for the entire system.

Steps

1. On the Canvas 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**.

Information		Features
Working Environment Tags	Tags	
Scheduled Downtime	Off	
S3 Storage Classes	Standard-Infrequent Access	
Instance Type	m5.xlarge	
Write Speed	Normal	
Ransomware Protection	Off	
Support Registration	Not Registered	
CIFs Setup		

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 BlueXP, 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 BlueXP. As a result, BlueXP cannot monitor the instance properly.

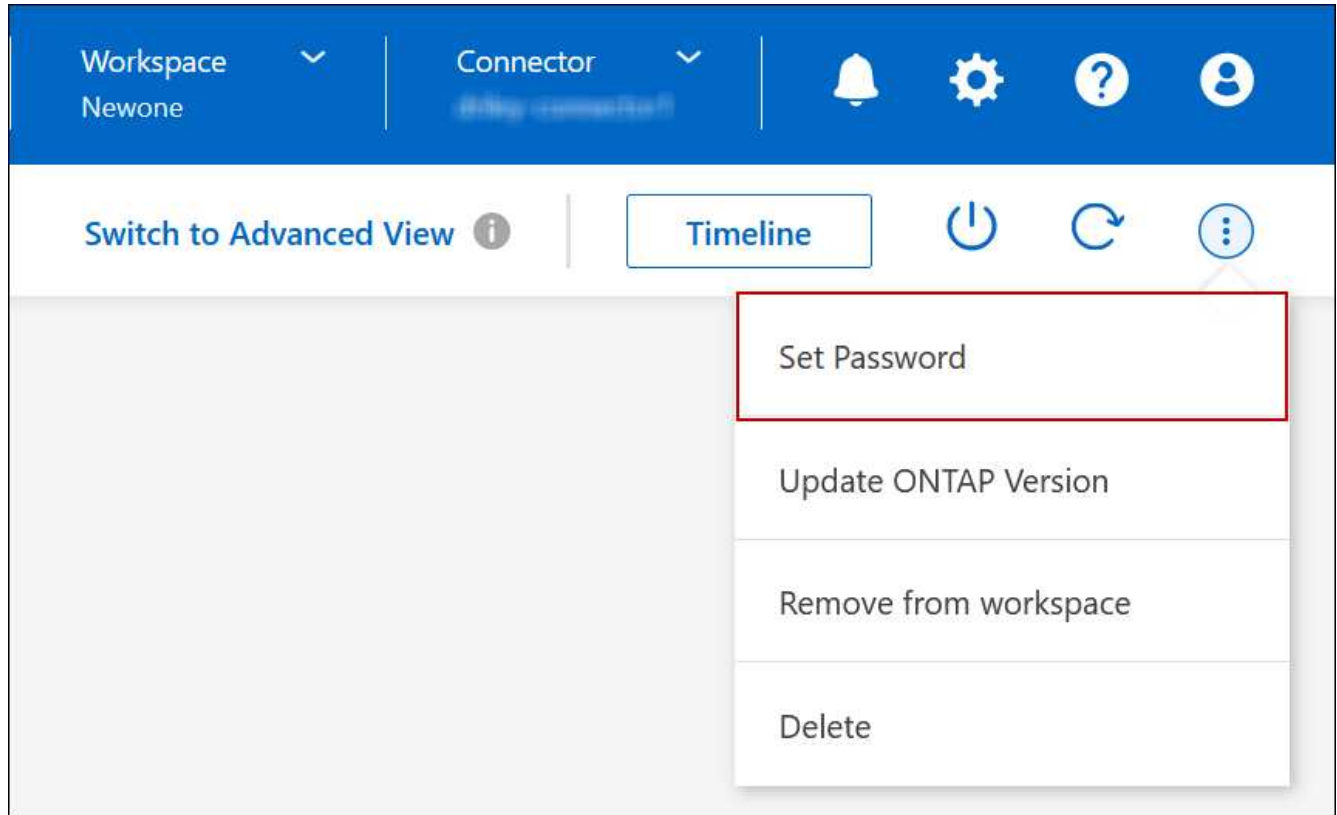
About this task

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 Canvas page, double-click the name of the Cloud Volumes ONTAP working environment.
2. On the upper right of the BlueXP console, click the ellipses icon, and select **Set password**.



Add, remove, or delete systems

Add an existing Cloud Volumes ONTAP system to BlueXP

You can discover and add existing Cloud Volumes ONTAP systems to BlueXP. You might do this if you deployed a new BlueXP system.

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 > Canvas**.
2. On the Canvas page, click **Add Working Environment**.
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

BlueXP adds the Cloud Volumes ONTAP instances to the project or workspace.

Remove a Cloud Volumes ONTAP working environment from BlueXP

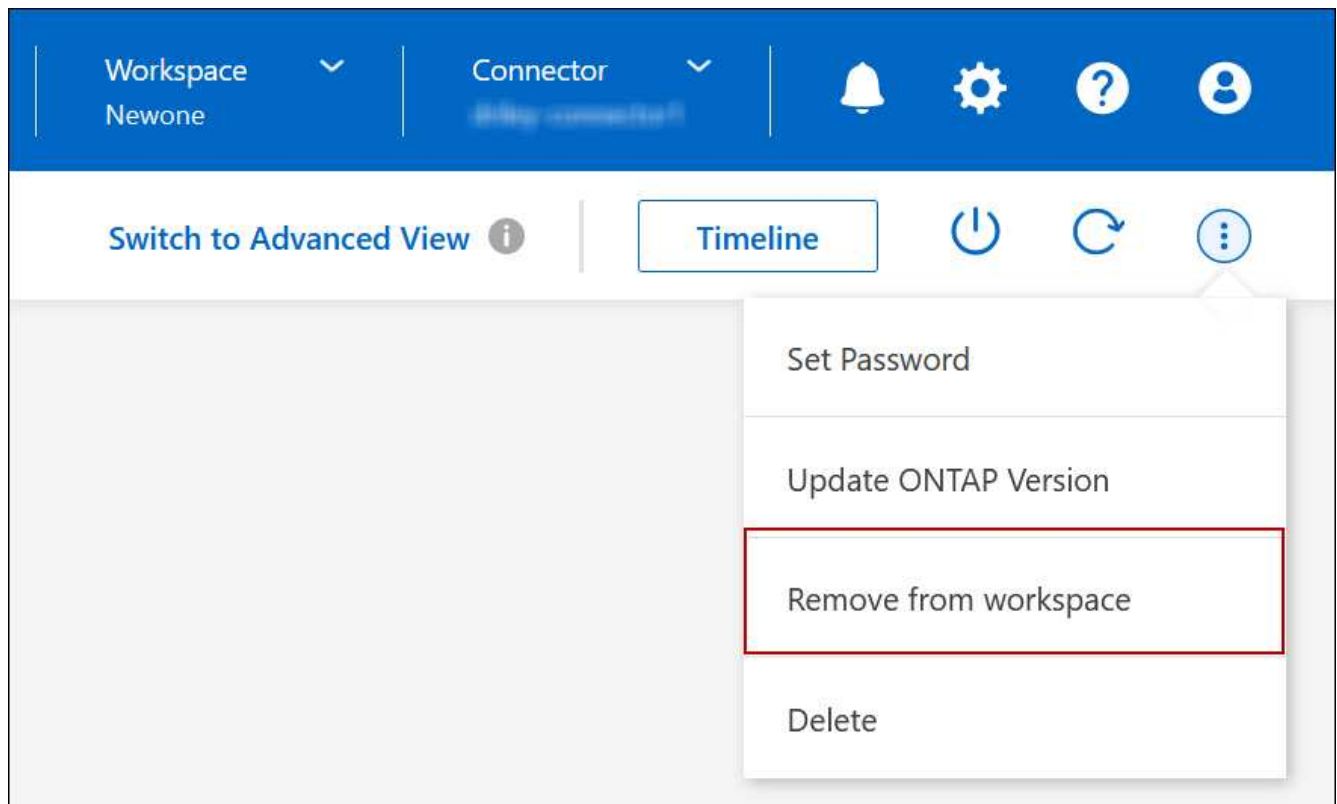
You can remove a Cloud Volumes ONTAP working environment to move it to another system or to troubleshoot discovery issues.

About this task

Removing a Cloud Volumes ONTAP working environment removes it from BlueXP. It does not delete the Cloud Volumes ONTAP system. You can later rediscover the working environment—for example, if you had problems during the initial discovery.

Steps

1. On the Canvas page, double-click on the working environment you want to remove.
2. On the upper right of the BlueXP console, click the ellipses icon, and select **Remove from workspace**.



3. In the Review from Workspace window, click **Remove**.

Result

BlueXP removes the working environment. Users can rediscover this working environment from the Canvas page at any time.

Delete a Cloud Volumes ONTAP system from BlueXP

You should always delete Cloud Volumes ONTAP systems from BlueXP, rather than from your cloud provider's console. For example, if you terminate a licensed Cloud Volumes ONTAP instance from your cloud provider, then you can't use the license key for another instance. You must delete the working environment from BlueXP to release the license.

When you delete a working environment, BlueXP terminates Cloud Volumes ONTAP instances and deletes disks and snapshots.



Other resources, such as backups managed by BlueXP backup and recovery, and instances for BlueXP classification, are not deleted when you delete a working environment. You'll need to manually delete them. If you don't, then you'll continue to incur charges for these resources.

When BlueXP deploys Cloud Volumes ONTAP in your cloud provider, it enables termination protection on the instances. This option helps prevent accidental termination.

Steps

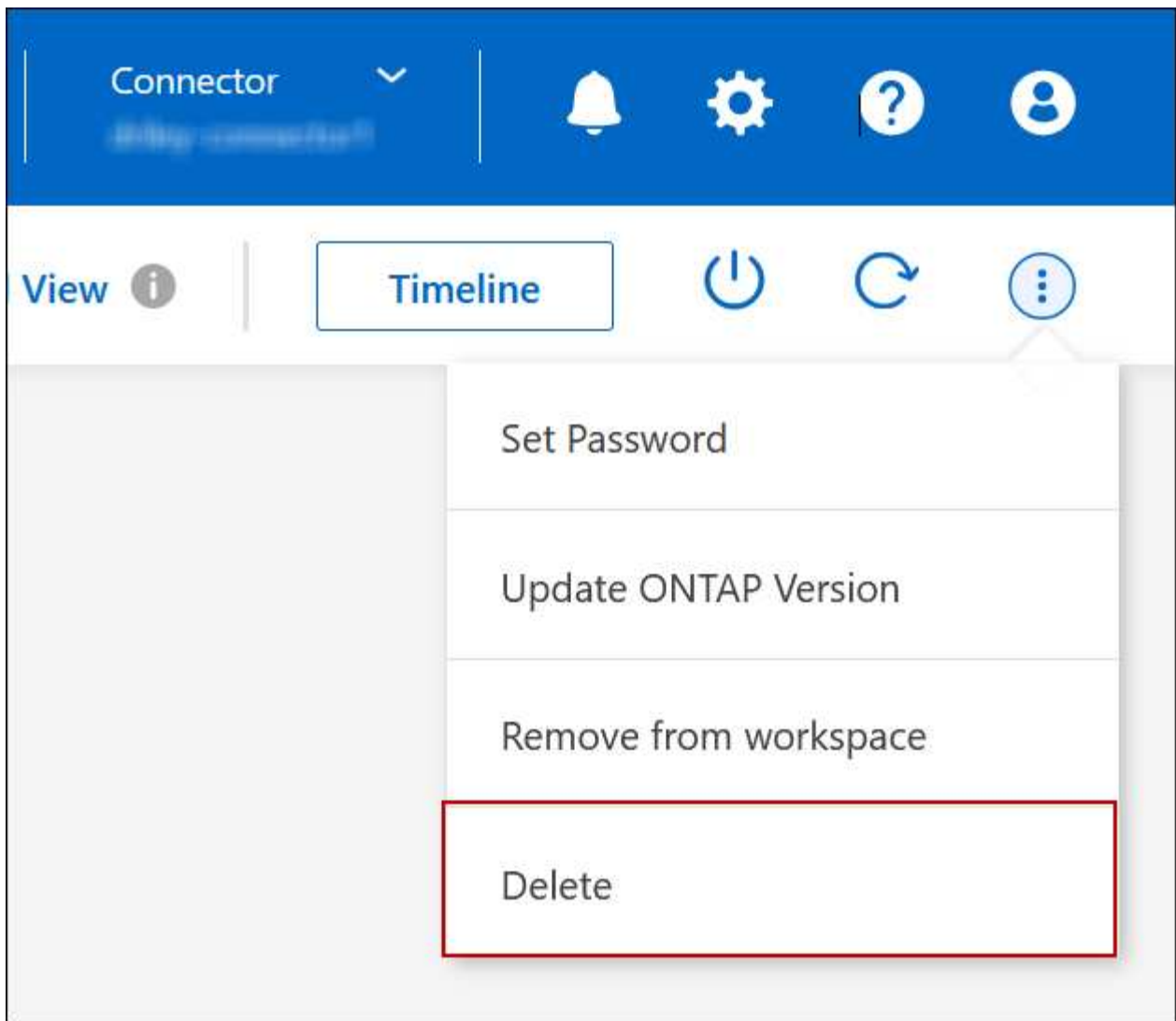
1. If you enabled BlueXP backup and recovery on the working environment, determine whether the backed up data is still required and then [delete the backups, if necessary](#).

BlueXP backup and recovery is independent from Cloud Volumes ONTAP by design. BlueXP 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 BlueXP classification on this working environment and no other working environments use this service, then you'll need to delete the instance for the service.

[Learn more about the BlueXP classification instance.](#)

3. Delete the Cloud Volumes ONTAP working environment.
 - a. On the Canvas page, double-click the name of the Cloud Volumes ONTAP working environment that you want to delete.
 - b. On the upper right of the BlueXP console, click the ellipses icon, and select **Delete**.



- c. Under the Delete Working Environment window, type the name of the working environment and then click **Delete**. It can take up to five minutes to delete the working environment.



BlueXP 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 BlueXP backup and recovery instance, you will be charged for the backed up copies until they are deleted.

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.

- Changing the VM type can affect Microsoft Azure service charges.
- The operation restarts Cloud Volumes ONTAP.

For single node systems, I/O is interrupted.

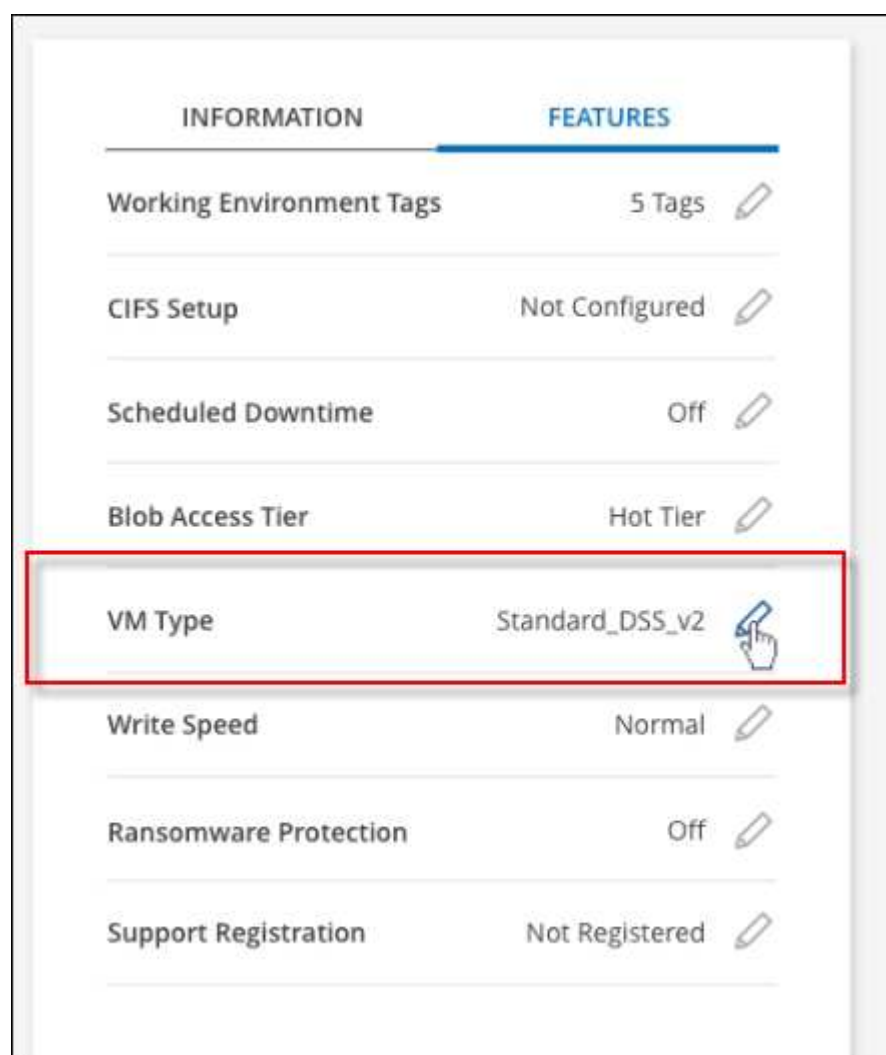
For HA pairs, the change is nondisruptive. HA pairs continue to serve data.



BlueXP 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 Canvas page, select the working environment.
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**.

1. 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 BlueXP Organization or Account admin can enable a setting in BlueXP 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.



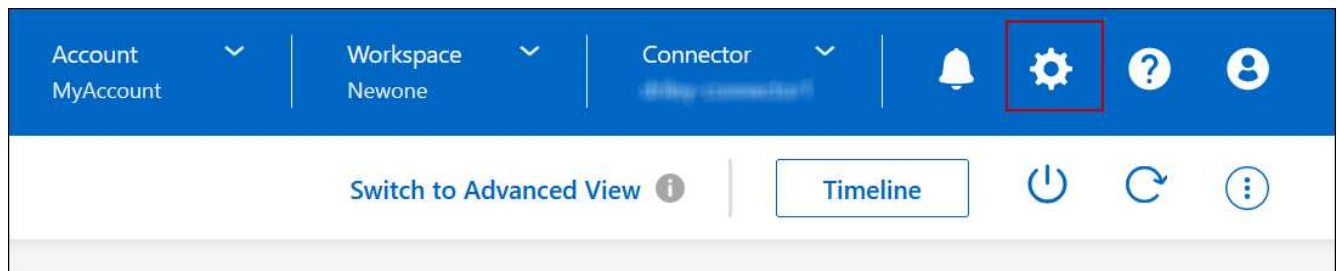
This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

Before you begin

You need to create a Connector before you can change BlueXP settings. [Learn how](#).

Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Cloud Volumes ONTAP Settings**.



2. Under **Azure**, click **Azure CIFS locks for Azure HA working environments**.
3. Click the checkbox to enable the feature and then click **Save**.

Use an Azure Private Link or service endpoints 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, BlueXP 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, BlueXP always limits network access for connections between Cloud Volumes ONTAP and storage accounts. Network access is limited to the VNet where Cloud Volumes ONTAP is deployed and the VNet where the Connector is deployed.

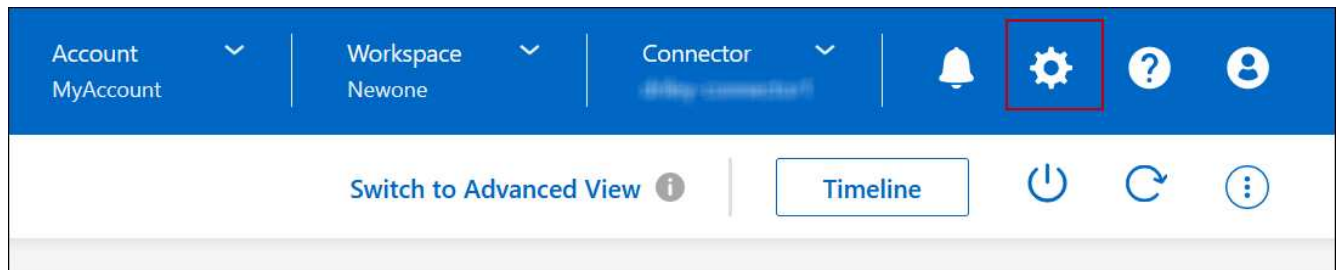
Disable Azure Private Links and use service endpoints instead

If required by your business, you can change a setting in BlueXP 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 Connector and Cloud Volumes ONTAP VNets.

The Connector should be deployed in the same Azure region as the Cloud Volumes ONTAP systems that it manages, or in the [Azure region pair](#) for the Cloud Volumes ONTAP systems.

Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Cloud Volumes ONTAP Settings**.



2. Under **Azure**, click **Use Azure Private Link**.
3. Deselect **Private Link connection between Cloud Volumes ONTAP and storage accounts**.
4. Click **Save**.

After you finish

If you disabled Azure Private Links and the Connector uses a proxy server, you must enable direct API traffic.

[Learn how to enable direct API traffic on the Connector](#)

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. BlueXP 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

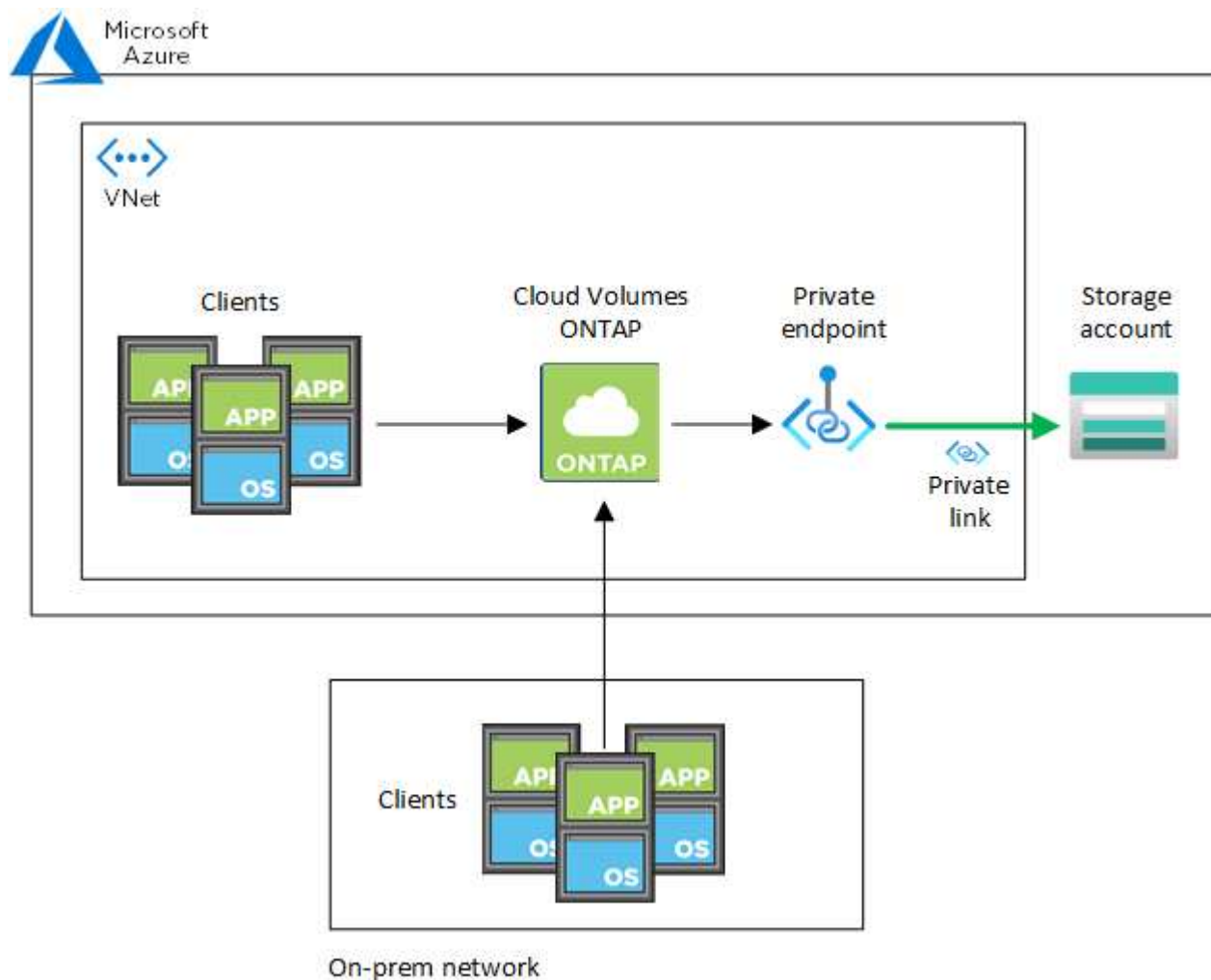
zone from your custom DNS servers. To learn more, refer to [Azure's documentation on using a DNS forwarder](#).

How Private Link connections work

When BlueXP 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 Connector and Cloud Volumes ONTAP systems are deployed in different VNets, then you must set up VNet peering between the VNet where the Connector is deployed and the VNet where the Cloud Volumes ONTAP systems are deployed.

Provide BlueXP with details about your Azure Private DNS

If you use [Azure Private DNS](#), then you need to modify a configuration file on each Connector. Otherwise, BlueXP can't enable the Azure Private Link connection between Cloud Volumes ONTAP and its associated

storage accounts.

Note that the DNS name must match Azure DNS naming requirements [as shown in Azure documentation](#).

Steps

1. SSH to the Connector host and log in.
2. Navigate to the `/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 Connector.

4. Save the file and log off the Connector.

A reboot isn't required.

Enable rollback on failures

If BlueXP fails to create an Azure Private Link as part of specific actions, it completes the action without the Azure Private Link connection. This can happen when creating a new working environment (single node or HA pair), or when the following actions occur on an HA pair: creating a new aggregate, adding disks to an existing aggregate, or creating a new storage account when going above 32 TiB.

You can change this default behavior by enabling rollback if BlueXP 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, BlueXP 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 Connector host and log in.
2. Navigate to the following directory: `/opt/application/netapp/cloudmanager/docker_occm/data`
3. Edit `app.conf` by adding the following parameter and value:

```
"rollback-on-private-link-failure": true
```

4. Save the file and log off the Connector.

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 working environment 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 working environment from **Canvas**.

To learn how to remove a working environment, refer to [Removing Cloud Volumes ONTAP working environments](#).

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. In **Canvas**, discover the working environment.
4. Look for the new resource group in the information for the working environment.

Result

The working environment 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.

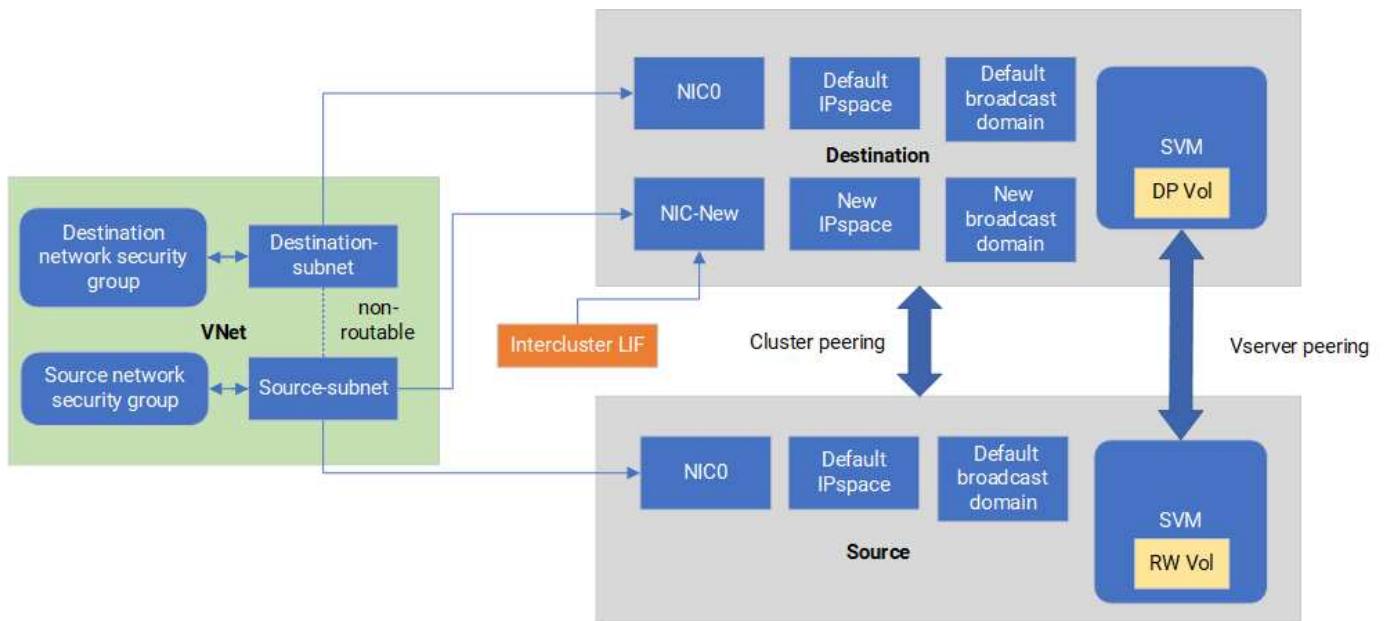
About SnapMirror traffic segregation in Azure

By default, BlueXP 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-addr`s. For HA pairs, list the source intercluster LIF IP address for both nodes as the `-peer-addr`s.

```
dest::> cluster peer create -peer-addr <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-addr`s. For HA pairs, list the destination intercluster LIF IP address for both nodes as the `-peer-addr`s.

```
src::> cluster peer create -peer-addr <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.

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 BlueXP.

Features

You can perform various storage management functions using ONTAP System Manager in BlueXP. 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. BlueXP 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.
- S3 object storage management: S3 storage management capabilities in Cloud Volumes ONTAP are available only in System Manager, and not in BlueXP.

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:

- BlueXP tiering: Cloud Volumes ONTAP does not support the BlueXP tiering service. You should set up tiering of data to object storage directly from BlueXP's Standard View when creating volumes.
- Tiers: Aggregate management (including local tiers and cloud tiers) is not supported from System Manager. You must manage aggregates directly from BlueXP's Standard View.
- Firmware upgrades: Cloud Volumes ONTAP does not support automatic firmware updates from the **Cluster > Settings** page.
- 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 BlueXP. 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 BlueXP or when the page is reloaded, because BlueXP doesn't store the credentials internally. If you disable authentication, users can access System Manager using BlueXP admin credentials.



This setting is applicable per BlueXP Connector for the ONTAP users in your organization or account, irrespective of Cloud Volumes ONTAP working environments or BlueXP projects.

Required permissions

You need to be assigned BlueXP Organization or Account admin privileges to modify the BlueXP Connector settings for Cloud Volumes ONTAP user authentication.

Steps

1. Select the **Connector** drop-down from the BlueXP header.
2. Select **Manage Connectors**.
3. Click the action menu **...** for the required Connector and select **Edit Connector**.
4. 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.

5. Click **Save**.

Get started with System Manager

You can access ONTAP System Manager from a Cloud Volumes ONTAP working environment.

Steps

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, select a Cloud Volumes ONTAP system.
3. From the right panel, select **Services > System Manager > Open**.
4. If prompted, enter your ONTAP user credentials and click **Login**.
5. If the confirmation message appears, read through it and click **Close**.
6. Use System Manager to manage Cloud Volumes ONTAP.
7. If needed, click **Switch to Standard View** to return to standard management through BlueXP.

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

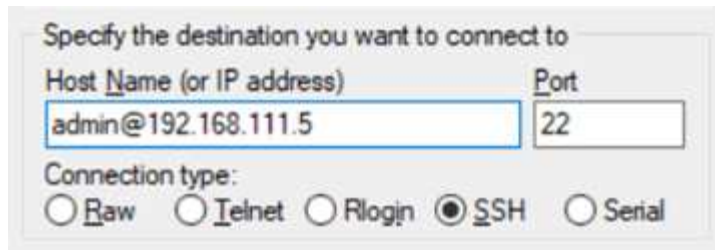
The host from which you use SSH to connect to Cloud Volumes ONTAP must have a network connection to Cloud Volumes ONTAP. For example, you might need to SSH from a jump host that's in your cloud provider network.

Steps

1. In BlueXP, identify the IP address of the cluster management interface:
 - a. From the left navigation menu, select **Storage > Canvas**.
 - b. On the Canvas 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://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

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

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



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 BlueXP can't configure your Cloud Volumes ONTAP system to use the Connector as a proxy server, you'll receive a notification from BlueXP titled "<working environment name> is unable to send AutoSupport messages."

You're most likely receiving this message because of networking issues.

Follow these steps to address this problem.

Steps

1. SSH to the Cloud Volumes ONTAP system so that you can administer the system from the ONTAP CLI.

[Learn how to SSH to Cloud Volumes ONTAP](#).

2. Display the detailed status of the AutoSupport subsystem:

```
autosupport check show-details
```

The response should be similar to the following:

```

Category: smtp
  Component: mail-server
    Status: failed
    Detail: SMTP connectivity check failed for destination:
            mailhost. Error: Could not resolve host -
'mailhost'
    Corrective Action: Check the hostname of the SMTP server

Category: http-https
  Component: http-put-destination
    Status: ok
    Detail: Successfully connected to:
            <https://support.netapp.com/put/AsupPut/>.

  Component: http-post-destination
    Status: ok
    Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

Category: on-demand
  Component: ondemand-server
    Status: ok
    Detail: Successfully connected to:
            https://support.netapp.com/aods/asupmessage.

Category: configuration
  Component: configuration
    Status: ok
    Detail: No configuration issues found.
5 entries were displayed.

```

If the status of the http-https category is "ok" then it means AutoSupport is configured properly and messages can be sent.

3. If the status is not ok, verify the proxy URL for each Cloud Volumes ONTAP node:

```
autosupport show -fields proxy-url
```

4. If the proxy URL parameter is empty, configure Cloud Volumes ONTAP to use the Connector as a proxy:

```
autosupport modify -proxy-url http://<connector private ip>:3128
```

5. Verify AutoSupport status again:

```
autosupport check show-details
```

6. If the status is still failed, validate that there is connectivity between Cloud Volumes ONTAP and the Connector over port 3128.
7. If the status ID is still failed after verifying that there is connectivity, SSH to the Connector.

[Learn more about Connecting to the Linux VM for the Connector](#)

8. Go to `/opt/application/netapp/cloudmanager/docker_occm/data/`
9. Open the proxy configuration file `squid.conf`

The basic structure of the file is as follows:

```
http_port 3128
acl localnet src 172.31.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

The `localnet` `src` value is the CIDR of the Cloud Volumes ONTAP system.

10. If the CIDR block of the Cloud Volumes ONTAP system isn't in the range that's specified in the file, either update the value or add a new entry as follows:

```
acl cvonet src <cidr>
```

If you add this new entry, don't forget to also add an allow entry:

```
http_access allow cvonet
```

Here's an example:

```
http_port 3128
acl localnet src 172.31.0.0/16
acl cvonet src 172.33.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access allow cvonet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

11. After editing the config file, restart the proxy container as `sudo`:

```
docker restart squid
```

12. Go back to the Cloud Volumes ONTAP CLI and verify that Cloud Volumes ONTAP can send AutoSupport messages:

```
autosupport check show-details
```

Configure EMS for Cloud Volumes ONTAP systems

Related links

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 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 BlueXP 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](#)

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, BlueXP 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 BlueXP 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 BlueXP backup and recovery, however no charges will be incurred for using this service. For more information on setting up licensing for BlueXP backup and recovery, refer to [Set up licensing for BlueXP 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 BlueXP Connector to be up and running. For more information, refer to [Learn about Connectors](#).



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](#).

How to get started

Learn how to get started with capacity-based licensing:

- [Set up licensing for Cloud Volumes ONTAP in Azure](#)

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 Azure](#)

Node-based licensing

Node-based licensing is the previous generation licensing model that enabled you to license Cloud Volumes

ONTAP by node. This licensing model is not available for new customers. 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

BlueXP 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

Capacity-based licensing packages are available with the following consumption models:

- **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 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

Pricing and supported configurations

For details about pricing, go to the [NetApp BlueXP website](#).

Capacity-based licensing packages are available with Cloud Volumes ONTAP 9.7 and later.

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.

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 BlueXP account. A *system* is a Cloud Volumes ONTAP HA pair, a Cloud Volumes ONTAP single node system, or any additional storage VMs that you create. The default storage VM does not count against the limit. This limit applies to all licensing models.

For example, let's say you have three working environments:

- A single node Cloud Volumes ONTAP system with one storage VM (this is the default storage VM that's created when you deploy Cloud Volumes ONTAP)

This working environment counts as one system.

- A single node Cloud Volumes ONTAP system with two storage VMs (the default storage VM, plus one additional storage VM that you created)

This working environment counts as two systems: one for the single node system and one for the additional storage VM.

- A Cloud Volumes ONTAP HA pair with three storage VMs (the default storage VM, plus two additional storage VMs that you created)

This working environment counts as three systems: one for the HA pair and two for the additional storage VMs.

That's six systems in total. You would then have room for an additional 14 systems in your account.

If you have a large deployment that requires more than 24 systems, contact your account rep or sales team.

[Learn more about BlueXP accounts.](#)

[Learn about storage limits for AWS, Azure, and Google Cloud.](#)

Notes about charging

The following details can help you understand how charging works with capacity-based licensing.

Minimum charge

There is a 4 TiB minimum charge for each data-serving storage VM that has at least one primary (read-write) volume. If the sum of the primary volumes is less than 4 TiB, then BlueXP 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.

Overages

If you exceed your BYOL capacity, you'll be charged for overages at hourly rates based on your marketplace subscription. Overages are charged at marketplace rates, with a preference for using available capacity from other licenses first. If your BYOL license expires, you need to transition to a capacity-based licensing model through cloud marketplaces.

Essentials package

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, BlueXP 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, BlueXP considers it as secondary data again and charges accordingly using the best matching license in the digital wallet.

- 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.

BYOL

If you purchased an Essentials license from NetApp (BYOL) and you exceed the licensed capacity for that deployment and volume type, the BlueXP digital wallet charges overages against a higher priced Essentials license (if you have one and there is available capacity). This happens because we first use the available capacity that you've already purchased as prepaid capacity before charging against the marketplace. If there is no available capacity with your BYOL license, the exceeded capacity will be charged at marketplace on-demand hourly rates (PAYGO) and will add costs to your monthly bill.

Here's an example. Let's say you have the following licenses for the Essentials package:

- A 500 TiB *Essentials Secondary HA* license that has 500 TiB of committed capacity
- A 500 TiB *Essentials Single Node* license that only has 100 TiB of committed capacity

Another 50 TiB is provisioned on an HA pair with secondary volumes. Instead of charging that 50 TiB to PAYGO, the BlueXP digital wallet charges the 50 TiB overage against the *Essentials Single Node* license. That license is priced higher than *Essentials Secondary HA*, but it's making use of a license you have already purchased, and it will not add costs to your monthly bill.

In the BlueXP digital wallet, that 50 TiB will be shown as 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 BlueXP digital wallet charges overages at the marketplace rate for the additional 100 TiB.

The overage charges will appear on your monthly bill.

Marketplace contracts or private offers

If you purchased an Essentials license as part of a marketplace contract or a private offer, the BYOL logic does not apply, and you must have the exact license type for the usage. License type includes volume type (primary or secondary) and the deployment type (HA or single node).

For example, let's say you deploy a Cloud Volumes ONTAP instance with the Essentials license. You then provision read-write volumes (primary single node) and read-only (secondary single node) volumes. Your marketplace contract or private offer must include capacity for *Essentials Single Node* and *Essentials Secondary Single Node* to cover the provisioned capacity. Any provisioned capacity that isn't part of your marketplace contract or private offer will be charged at the on-demand hourly rates (PAYGO) and will add costs to 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 cloud providers. BlueXP 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

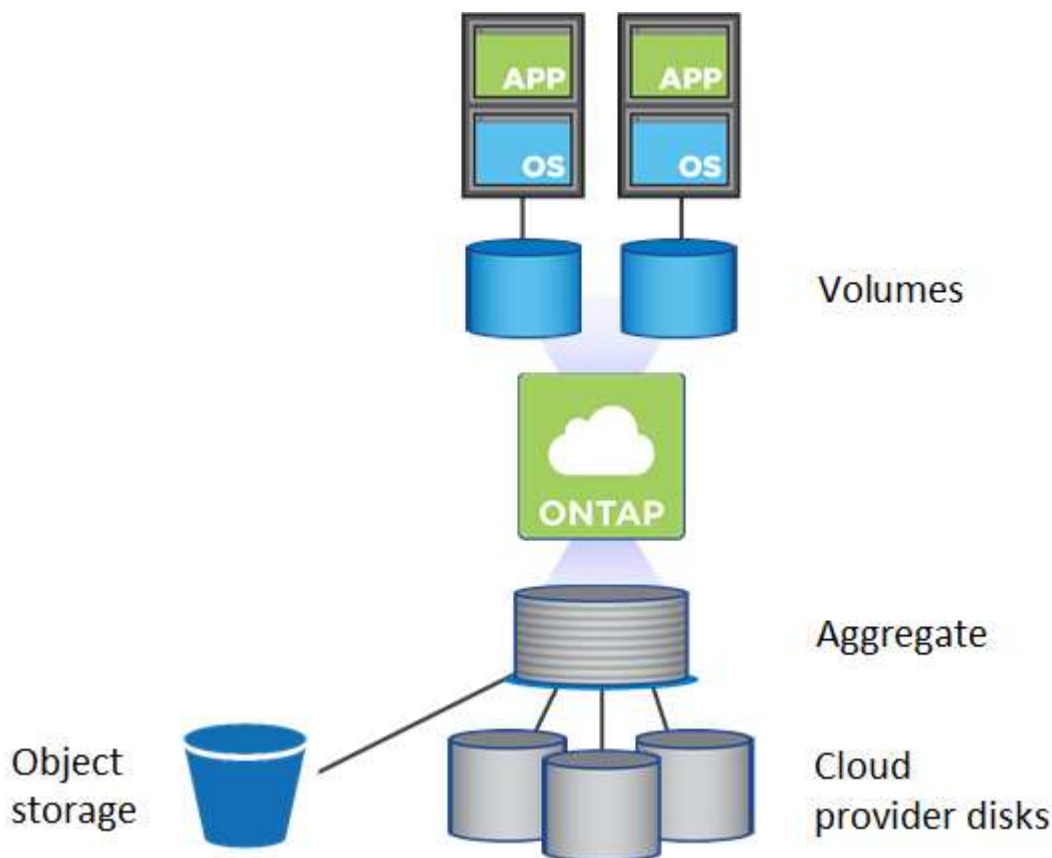
Understanding how Cloud Volumes ONTAP uses cloud storage can help you understand your storage costs.



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

Overview

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



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



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

Azure storage

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

Single node systems

Single node systems can use 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](#)

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

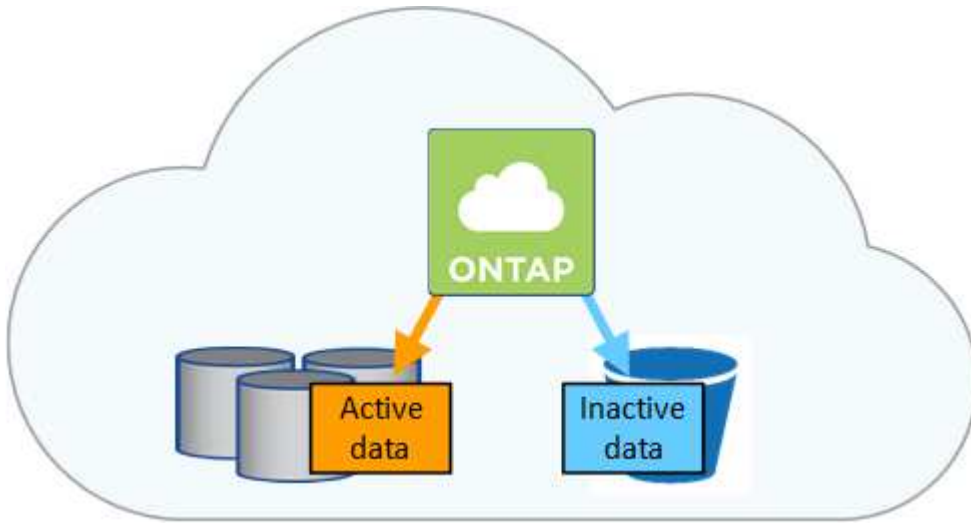
RAID0 doesn't support the use of hot spares for redundancy.

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 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 Azure

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

Performance tier

The performance tier can be either SSDs or HDDs.

Capacity tier

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

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

BlueXP creates the storage account with the following settings:

- Access tier: Hot
- Performance: Standard
- Redundancy: 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 create the working environment 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 and capacity limits

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

Volume tiering policies

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

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



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

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

Snapshot Only

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

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

All

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

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

Auto

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

This policy is supported starting with Cloud Volumes ONTAP 9.4.

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

None

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

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

Turning off Cloud Volumes ONTAP impacts the cooling period

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

- Auto: 31 days
- Snapshot Only: 2 days

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



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

Setting up data tiering

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

Cloud Volumes ONTAP storage management

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



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

Storage provisioning

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

provision aggregates yourself, if desired.

Simplified provisioning

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

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

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

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

Advanced allocation

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

Capacity management

The BlueXP Organization or Account admin can choose whether BlueXP notifies you of storage capacity decisions or whether BlueXP automatically manages capacity requirements for you.

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

Automatic capacity management

The Capacity Management Mode is set to automatic by default. In this mode, BlueXP 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, BlueXP automatically 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, BlueXP automatically purchases new disks for that aggregate so volumes can continue to grow.
- If an aggregate reaches the capacity threshold and it can't support any additional disks, BlueXP automatically moves a volume from that aggregate to an aggregate with available capacity or to a new aggregate.

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

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

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

Management of LUNs with automatic capacity management

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

Manual capacity management

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

Learn more

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

Write speed

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

Normal write speed

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

Normal write speed is the default option.

High write speed

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

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

When to use high write speed

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

Recommendations when using high write speed

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

Configurations that support high write speed

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

Azure

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

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

How to select a write speed

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

What to expect if data loss occurs

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

- Cloud Volumes ONTAP 9.12.1 or later

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

- Cloud Volumes ONTAP 9.11.0 to 9.11.1

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

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

- Cloud Volumes ONTAP 9.8 to 9.10.1

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

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


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

How to stop data access if data loss occurs

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

To enable the NVFAIL option

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

To check NVFAIL settings

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

To disable the NVFAIL option

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

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

To check the NVFAIL state

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

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

To clear the NVFAIL state

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

Flash Cache

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

What's Flash Cache?

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

Supported configurations

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

Limitations

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

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

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

You can enable WORM storage when creating a Cloud Volumes ONTAP working environment on BlueXP. You can also enable WORM on a working environment 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 Canvas page, double-click the name of the working environment 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](#)

High-availability pairs

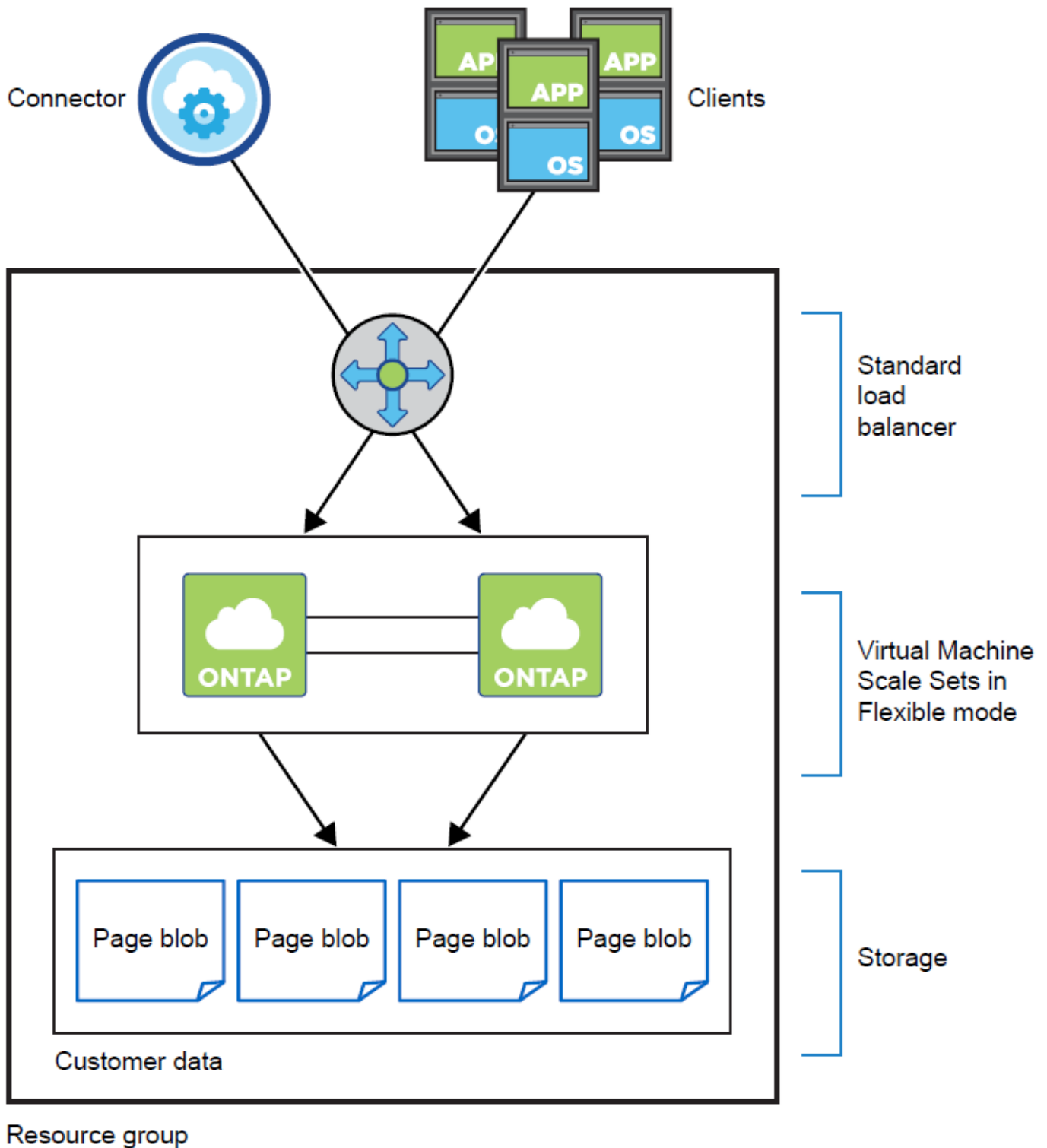
Learn about Cloud Volumes ONTAP HA pairs in Azure

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 BlueXP 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 [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 BlueXP creates for HA pairs are general-purpose v2 storage accounts.
- You can enable an HTTPS connection from a Cloud Volumes ONTAP 9.7 HA pair to Azure storage accounts when creating a working environment. Note that enabling this option can impact write performance. You can't change the setting after you create the working environment.

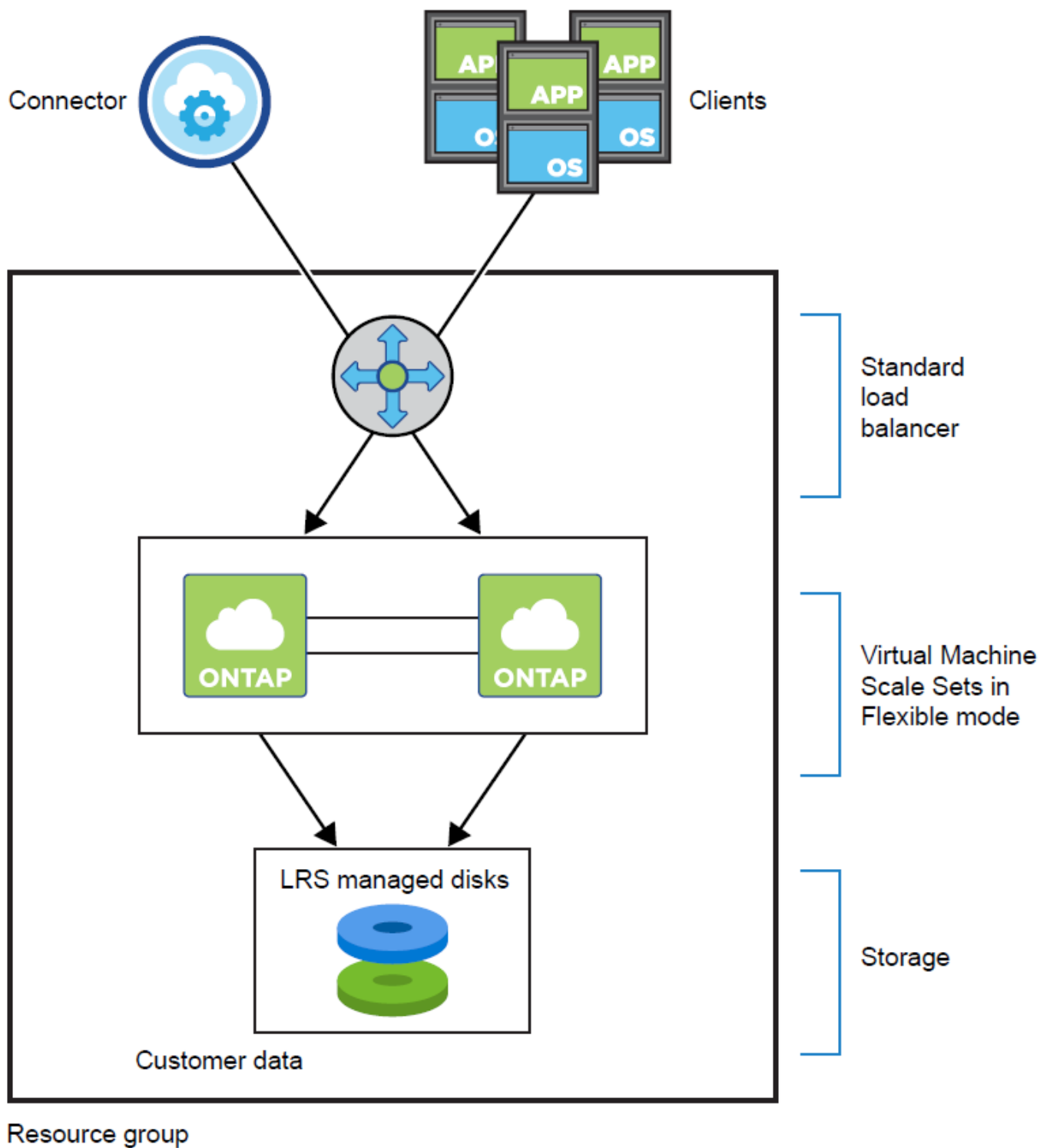


Starting with Cloud Volumes ONTAP 9.15.0P1, Azure page blobs are no longer supported for new high-availability pair deployments. If you currently use Azure page blobs in existing high-availability pair deployments, you can migrate to newer VM instance types in the Edsv4-series VMs and Edsv5-series VMs.

[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 BlueXP 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 [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](#).

Disks

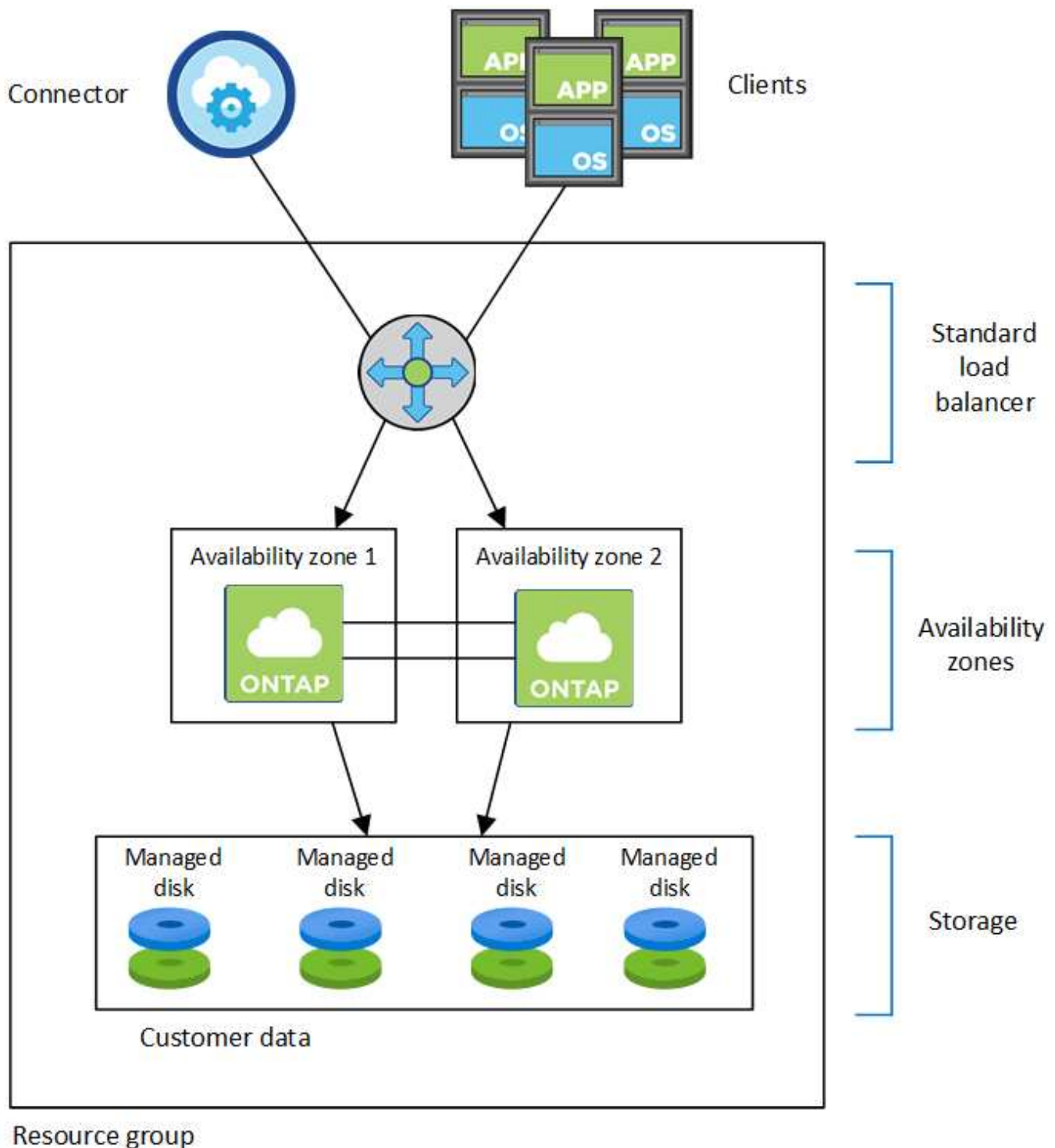
Customer data resides on locally-redundant storage (LRS) managed disks. Each node has access to the other node's storage. Additional storage is also required for [boot](#), [root](#), [partner root](#), [core](#), and [NVRAM data](#).

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 BlueXP 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 [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.

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 working environment in BlueXP is *Degraded*.

The following actions are unavailable from BlueXP storage takeover:

- Support registration
- License changes
- Instance or VM type changes
- Write speed changes
- CIFS setup
- Changing the location of configuration backups
- Setting the cluster password
- Managing disks and aggregates (advanced allocation)

These actions are available again after storage giveback completes and the state of the working environment changes back to normal.

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)
- Azure Storage Service Encryption

You can use NetApp encryption solutions with native encryption from your cloud provider, which encrypts data at the hypervisor level. Doing so would provide double encryption, which might be desired for very sensitive data. When the encrypted data is accessed, it's unencrypted twice—once at the hypervisor-level (using keys from the cloud provider) and then again using NetApp encryption solutions (using keys from an external key manager).

NetApp encryption solutions (NVE and NAE)

Cloud Volumes ONTAP supports [NetApp Volume Encryption \(NVE\)](#) and [NetApp Aggregate Encryption \(NAE\)](#). NVE and NAE are software-based solutions that enable (FIPS) 140-2-compliant data-at-rest encryption of volumes. Both NVE and NAE use AES 256-bit encryption.

- NVE encrypts data at rest one volume at 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 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:

- Azure Key Vault (AKV)

New aggregates have NetApp Aggregate Encryption (NAE) enabled by default after you set up an external key manager. New volumes that aren't part of an NAE aggregate 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](#).

Azure Storage Service Encryption

Data is automatically encrypted on Cloud Volumes ONTAP in Azure using [Azure Storage Service Encryption](#) with a Microsoft-managed key.

You can use your own encryption keys if you prefer. [Learn how to set up Cloud Volumes ONTAP to use a customer-managed key in Azure](#).

ONTAP virus scanning

You can use integrated antivirus functionality on ONTAP systems to protect data from being compromised by viruses or other malicious code.

ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

For information about the vendors, software, and versions supported by Vscan, 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. BlueXP enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

- BlueXP 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.

- BlueXP also enables you to block common ransomware file extensions by enabling ONTAP's FPolicy solution.

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection ⓘ




50 %
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes ⓘ

Activate Snapshot Policy

2 Block Ransomware File Extensions ⓘ



ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names ⓘ

Activate FPolicy

[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 Microsoft Azure

[NetApp Technical Report 4671: Performance Characterization of Cloud Volumes ONTAP in Azure with Application Workloads](#)

CPU performance

Cloud Volumes ONTAP nodes show as highly utilized (over 90%) from your cloud provider's monitoring tools. This is because ONTAP reserves all vCPUs presented to the virtual machine so that they are available when needed.

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. BlueXP 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 ONTAP](#).

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, BlueXP prompts you for the serial number of your license and your NetApp Support Site account. BlueXP 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 BlueXP.](#)

If BlueXP can't access the license file over the secure internet connection, you can [obtain the file yourself and then manually upload the file to BlueXP](#).

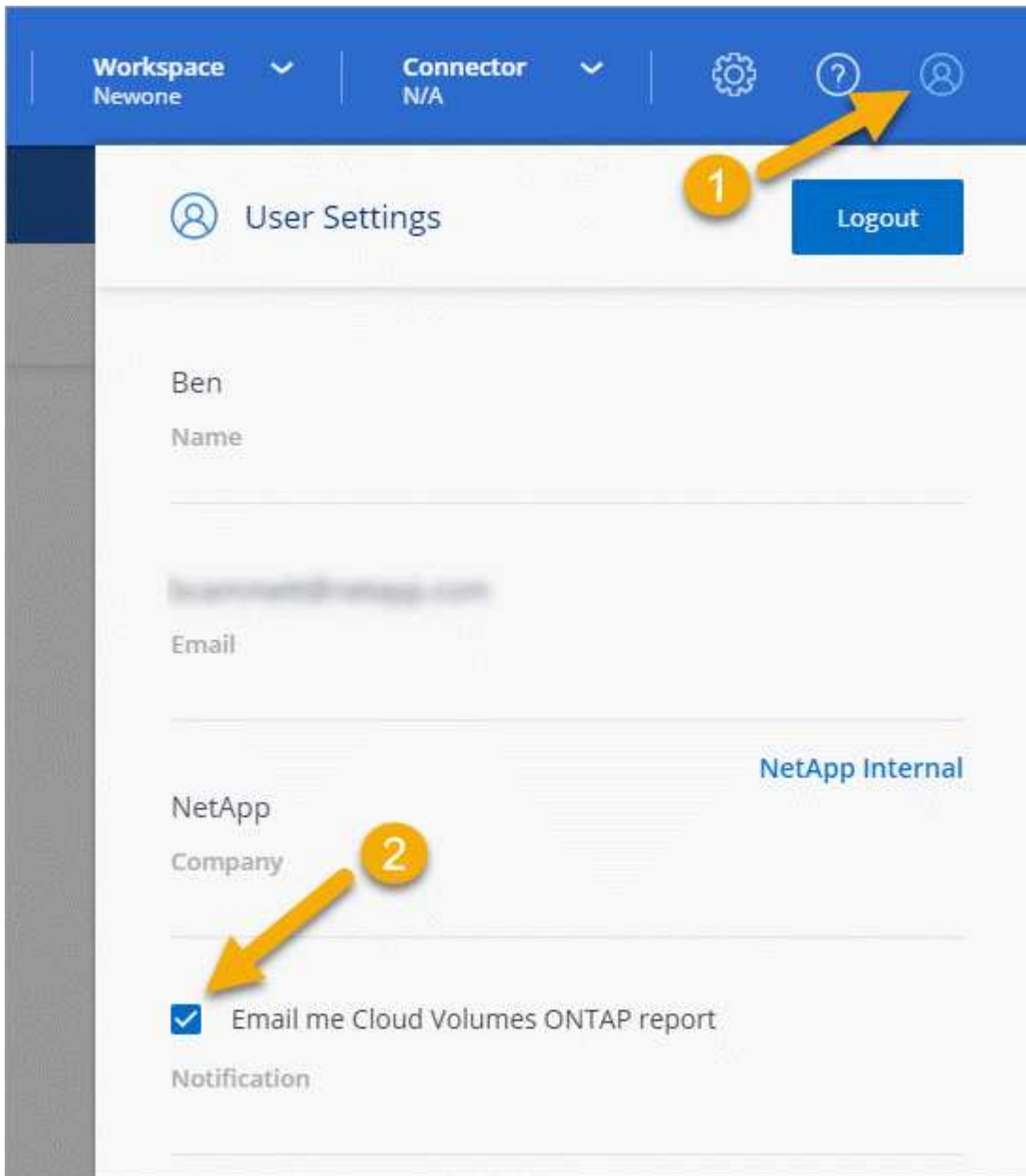
License expiration

BlueXP displays a warning 30 days before a node-based license is due to expire and again when the license expires. The following image shows a 30-day expiration warning that appears in the user interface:



You can select the working environment to review the message.

BlueXP includes a license expiration warning in the Cloud Volumes ONTAP report that's emailed to you, if you are a BlueXP 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, BlueXP automatically obtains the new license from NetApp and installs it on the Cloud Volumes ONTAP system.

If BlueXP can't access the license file over the secure internet connection, you can [obtain the file yourself and then manually upload the file to BlueXP](#).

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

- BlueXP creates one data-serving storage VM when it deploys Cloud Volumes ONTAP. Some configurations support additional storage VMs. [Learn more about managing storage VMs.](#)

Starting with the BlueXP 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?](#)

- BlueXP 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 9.9.1 in Azure

- SnapMirror
 - SnapRestore
 - SnapVault
- Several network interfaces are created by default:
 - A cluster management LIF
 - An intercluster LIF
 - An SVM management LIF on HA systems in Azure
 - A node management LIF
 - An iSCSI data LIF
 - A CIFS and NFS data LIF



LIF failover is disabled by default for Cloud Volumes ONTAP due to cloud provider requirements. Migrating a LIF to a different port breaks the external mapping between IP addresses and network interfaces on the instance, making the LIF inaccessible.


- Cloud Volumes ONTAP sends configuration backups to the Connector using HTTP.

The backups are accessible from `http://ipaddress/occm/offboxconfig/` where *ipaddress* is the IP address of the Connector host.

You can use the backups for reconfiguring your Cloud Volumes ONTAP system. For more information about configuration backups, refer to the [ONTAP documentation](#).

- BlueXP 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 that BlueXP sets differently from the defaults:

Attribute	Value set by BlueXP
Autosize mode	grow
Maximum autosize	1,000 percent <div>  <div>The BlueXP Organization or Account admin can modify this value from the Settings page.</div> </div>
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, BlueXP also purchases cloud storage for system data.

Azure (single node)

- Three Premium SSD disks:
 - One 10 GiB disk for boot data
 - One 140 GiB disk for root data
 - One 512 GiB disk for NVRAM

If the virtual machine that you chose for Cloud Volumes ONTAP supports Ultra SSDs, then the system uses a 32 GiB Ultra SSD for NVRAM, rather than a Premium SSD.

- One 1024 GiB Standard HDD disk for saving cores
- One Azure snapshot for each boot disk and root disk
- 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.

Where the disks reside

BlueXP lays out the storage as follows:

- Boot data resides on a disk attached to the instance or virtual machine.

This disk, which contains the boot image, is not available to Cloud Volumes ONTAP.

- Root data, which contains the system configuration and logs, resides in aggr0.
- The storage virtual machine (SVM) root volume resides in aggr1.
- Data volumes also reside in aggr1.

Knowledge and support

Register for support

Support registration is required to receive technical support specific to BlueXP and its storage solutions and 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 BlueXP 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 BlueXP account serial number (your 20 digit 960xxxxxxx serial number located on the Support Resources page in BlueXP).

This serves as your single support subscription ID for any service within BlueXP. Each BlueXP account-level support subscription must be registered.

- Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider's marketplace (these are 20 digit 909201xxxxxxx serial numbers).

These serial numbers are commonly referred to as *PAYGO serial numbers* and get generated by BlueXP 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 BlueXP as described below.

Register BlueXP for NetApp support

To register for support and activate support entitlement, one user in your BlueXP organization (or account) must associate a NetApp Support Site account with their BlueXP 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 BlueXP.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **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 BlueXP organization is registered for support.

Note that other BlueXP users will not see this same support registration status if they have not associated a NetApp Support Site account with their BlueXP login. However, that doesn't mean that your BlueXP organization is not registered for support. As long as one user in the organization has followed these steps, then your organization 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 BlueXP login.

Steps

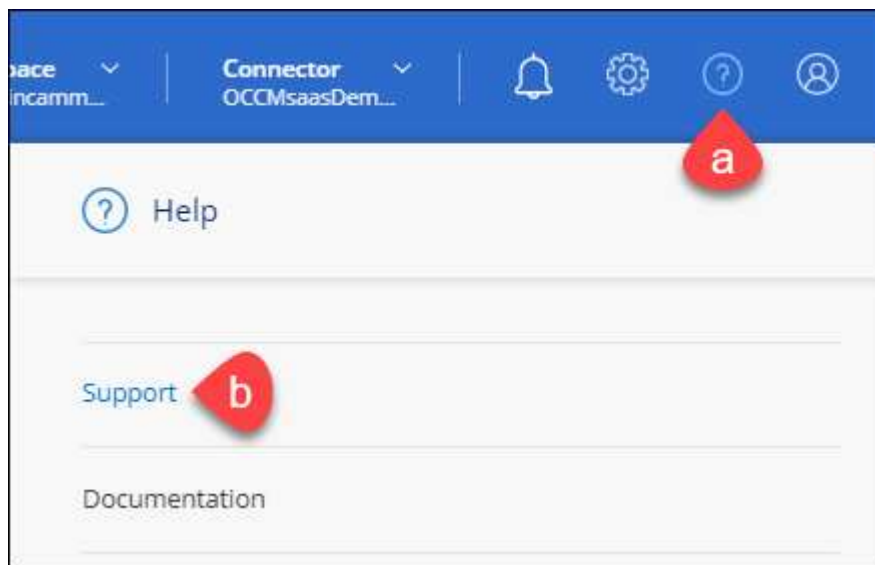
1. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
 - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
 - b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.
2. Associate your new NSS account with your BlueXP 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 BlueXP console, select the Help icon, and select **Support**.



2. Locate your account ID serial number from the Support Registration page.



96015585434285107893
Account serial number

⚠ Not Registered

Add your NetApp Support Site (NSS) [credentials](#) to BlueXP
Follow these [instructions](#) to register for support in case you don't have an NSS account yet.

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 BlueXP 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 BlueXP organization 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 BlueXP 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

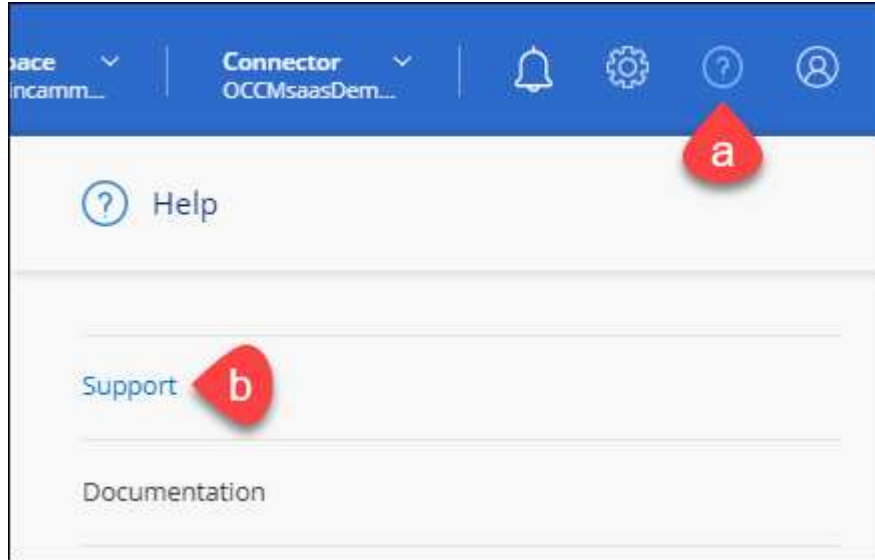
Associating NSS credentials with your BlueXP organization is different than the NSS account that is associated with a BlueXP user login.

These NSS credentials are associated with your specific BlueXP organization ID. Users who belong to the BlueXP 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 BlueXP 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 BlueXP 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 BlueXP and its cloud services in a variety of ways. Extensive free self-support options are available 24/7, such as knowledgebase (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 "Getting help" in the BlueXP documentation for that product.

- [Amazon FSx for ONTAP](#)
- [Azure NetApp Files](#)
- [Google Cloud NetApp Volumes](#)

To receive technical support specific to BlueXP and its storage solutions and 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 BlueXP documentation that you're currently viewing.

- [Knowledge base](#)

Search through the BlueXP knowledge base to find helpful articles to troubleshoot issues.

- [Communities](#)

Join the BlueXP 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 BlueXP login. [Learn how to manage credentials associated with your BlueXP 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 BlueXP, 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, BlueXP when specific to a technical support issue with workflows or functionality within the service.
 - **Working Environment:** If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.

The list of working environments are within scope of the BlueXP organization (or account), project (or workspace), and Connector you have selected in the top banner of the service.

- **Case Priority:** Choose the priority for the case, which can be Low, Medium, High, or Critical.

To learn more details about these priorities, hover your mouse over the information icon next to the field name.

- **Issue Description:** Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.
- **Additional Email Addresses:** Enter additional email addresses if you'd like to make someone else aware of this issue.
- **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.

ntapitdemo
NetApp Support Site Account

Service

Select

Working Enviroment

Select

Case Priority

Low - General guidance

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional)

Type here

Attachment (Optional)

No files selected

Upload

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 BlueXP account serial number (ie. 960xxxx) or the working environment serial number. You can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at <https://mysupport.netapp.com/site/help>

Manage your support cases (Preview)

You can view and manage active and resolved support cases directly from BlueXP. You can manage the cases associated with your NSS account and with your company.

Case management is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

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 BlueXP, select **Help > Support**.
2. Select **Case Management** and if you're prompted, add your NSS account to BlueXP.

The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP 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.

Search icon Cases opened on the last 3 months Create a case

Date created	Last updated		Status (5)	
December 22, 2022	December 29, 2022	Last 7 days	Assigned	...
December 21, 2022	December 28, 2022	Last 30 days	Active	...
December 15, 2022	December 27, 2022	Last 3 months	Pending customer	...
December 14, 2022	December 26, 2022	Medium (P3)	Solution proposed	...
		Low (P4)		

Apply Reset

- Filter the contents of the columns.

Search icon Cases opened on the last 3 months Create a case

Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	Active	...
December 28, 2022	High (P2)	Pending customer	...
December 27, 2022	Medium (P3)	Solution proposed	...
December 26, 2022	Low (P4)	Pending closed	...
		Closed	...

Apply Reset

- Change the columns that appear in the table by selecting  and then choosing the columns that you'd like to display.

Search icon Cases opened on the last 3 months Create a case

Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	Last updated	...
December 28, 2022	High (P2)	Priority	...
December 27, 2022	Medium (P3)	Cluster name	...
December 26, 2022	Low (P4)	Case owner	...
		Opened by	...

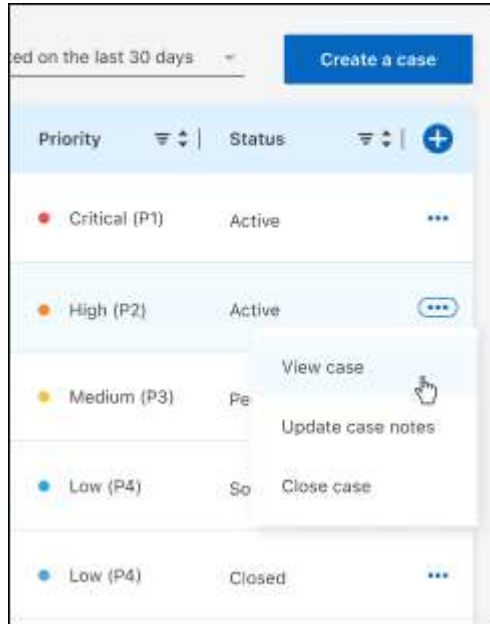
Apply Reset

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 BlueXP](#)
- [Notice for the Cloud Volumes ONTAP](#)
- [Notice for ONTAP](#)

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.