Use Cloud Volumes ONTAP

Cloud Volumes ONTAP

NetApp
August 19, 2025

This PDF was generated from https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-manage-capacity-licenses.html on August 19, 2025. Always check docs.netapp.com for the latest.

Table of Contents

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.

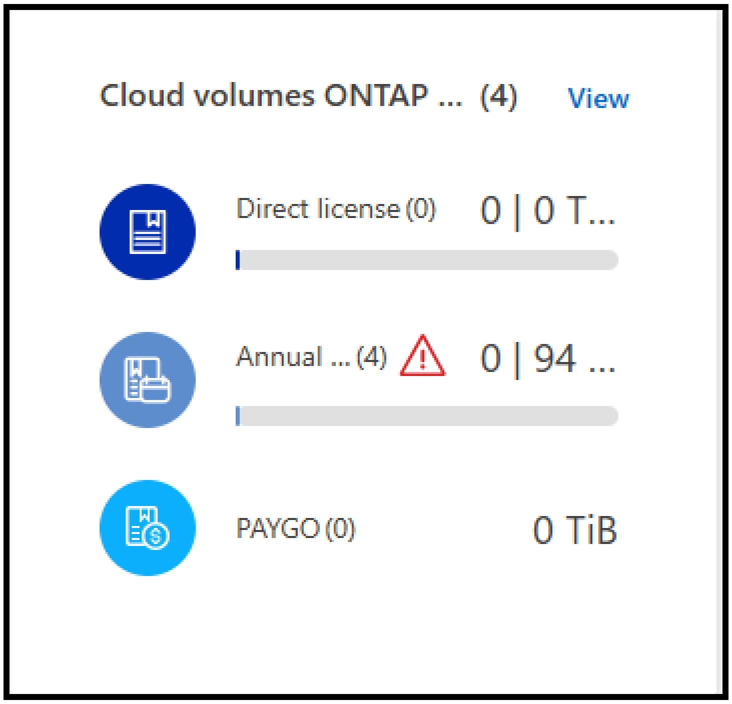
If BlueXP can't add the license, you'll need to manually add them to the digital wallet yourself. For example, if the Connector is installed in a location that doesn't have internet access, you'll need to add the licenses yourself. Learn how to add purchased licenses to your account.

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.



Cloud volumes ONTAP ... (4) View

Direct license (0) 0 | 0 T...

Annual ... (4) ⚠ 0 | 94 ...

PAYGO (0) 0 TiB

- *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.

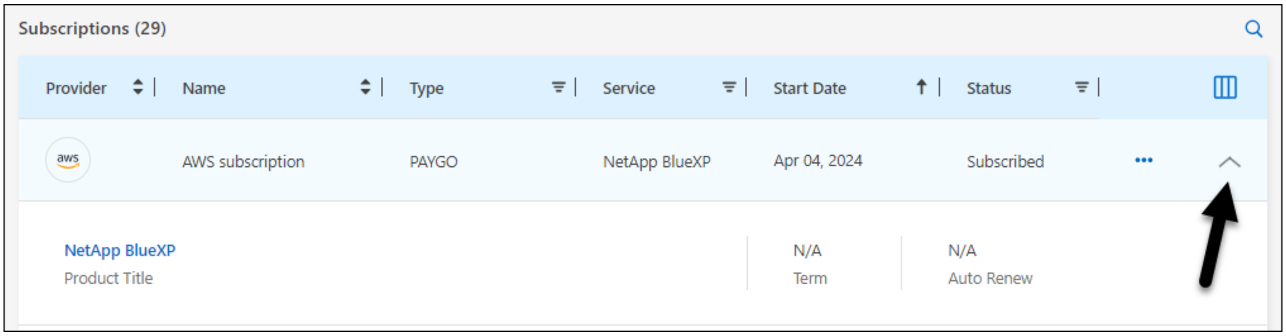
3. Select **View** to see the consumed capacity for each of your licensing packages.
4. Select the **Licenses** tab to see details for each package license that you have purchased.

   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.



Subscriptions (29)

Provider	Name	Type	Service	Start Date	Status	
aws	AWS subscription	PAYGO	NetApp BlueXP	Apr 04, 2024	Subscribed	•••

NetApp BlueXP
Product Title

N/A
Term

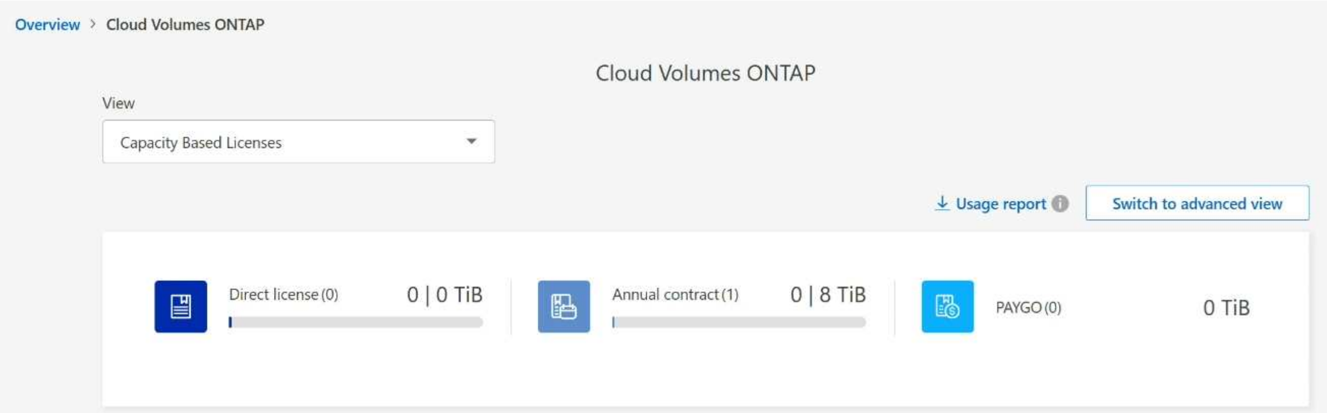
N/A
Auto Renew

- 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

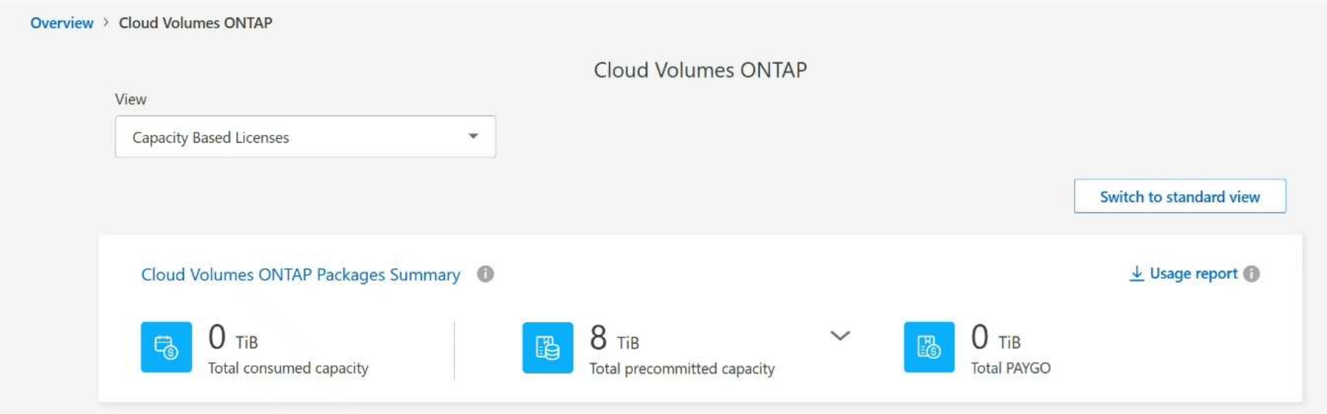
View: Capacity Based Licenses

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

Cloud Volumes ONTAP Packages Summary

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

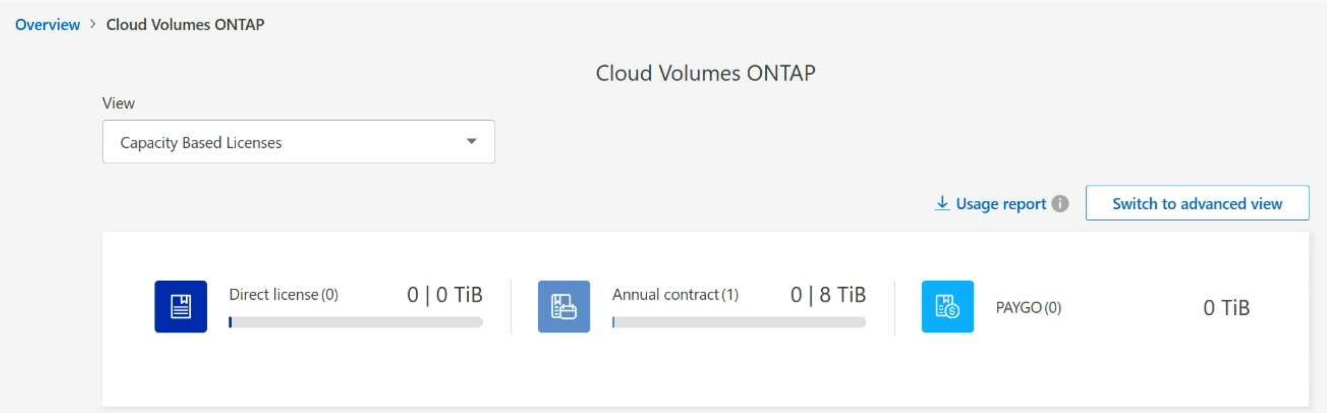
- Changing the charging method doesn't affect whether you're charged through a license purchased from NetApp (BYOL) or from your cloud provider's marketplace pay-as-you-go (PAYGO) subscription.

  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.

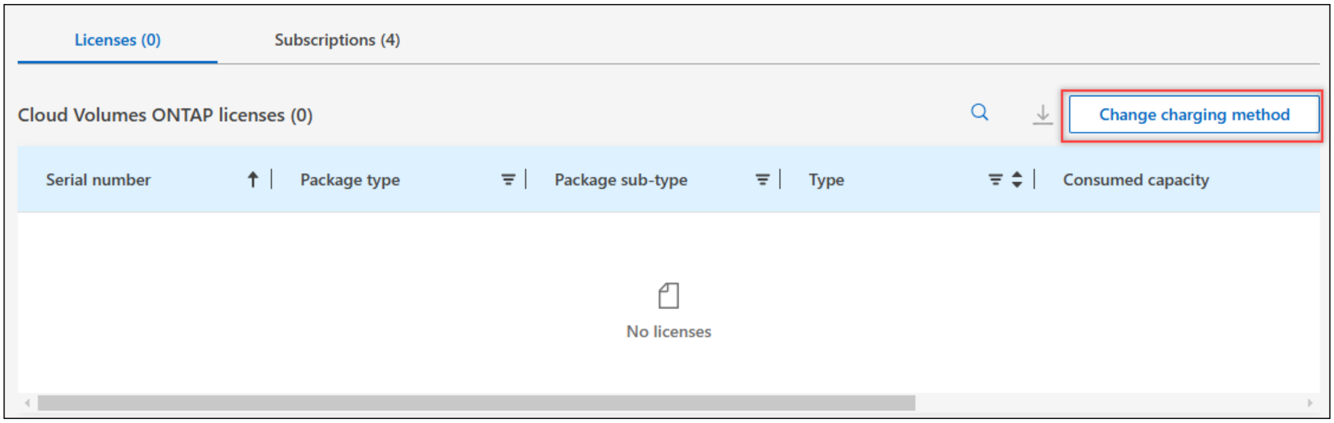
- If you have a private offer or contract from your cloud provider's marketplace, changing to a charging method that's not included in your contract will result in charging against BYOL (if you purchased a license from NetApp) or PAYGO.

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**.



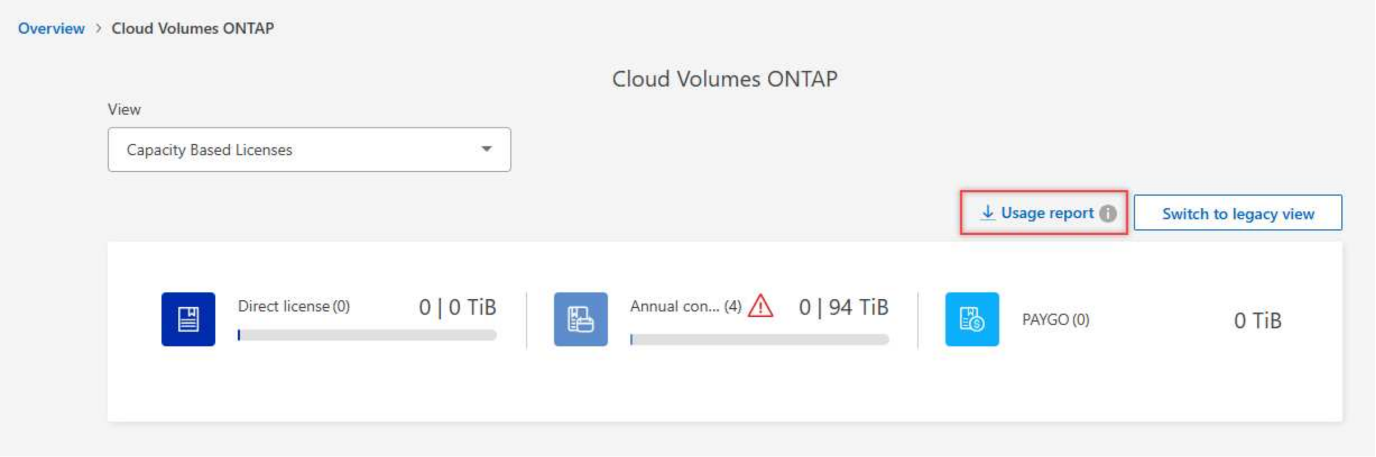
5. Scroll down to the **Capacity-based license** table and select **Change charging method**.



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.



View: Capacity Based Licenses

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

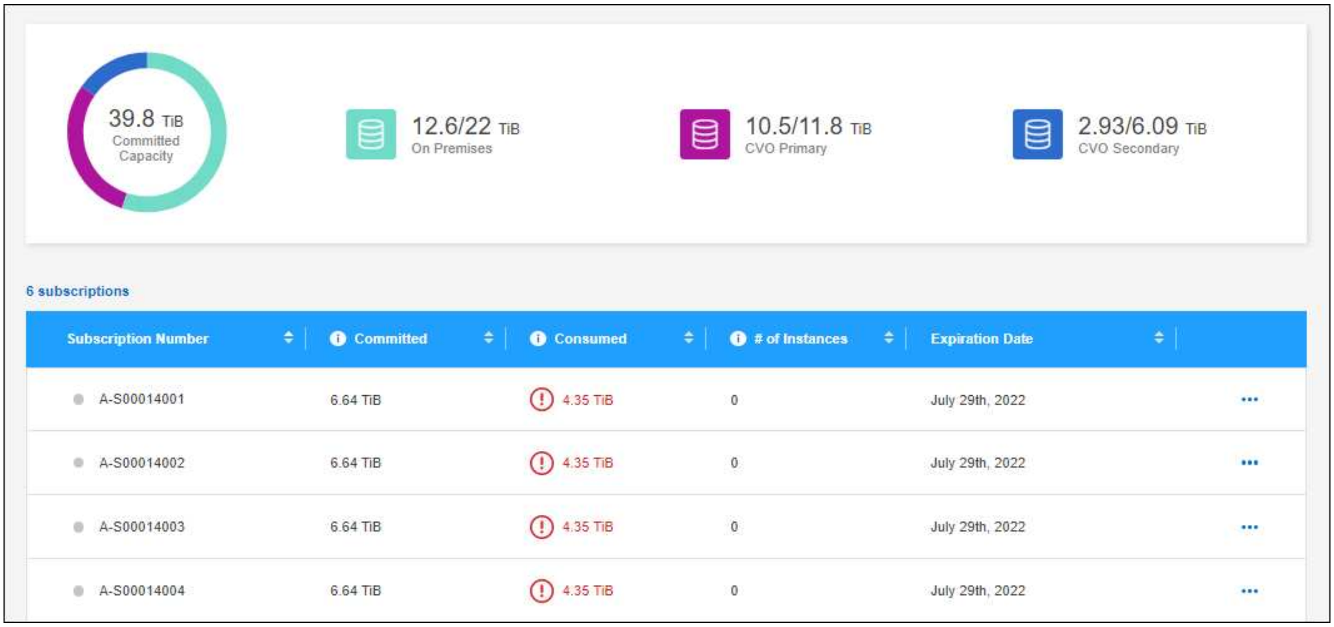
Before you can use and manage Keystone subscriptions in BlueXP, you need to contact NetApp to authorize your BlueXP user account with your Keystone subscriptions.

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.



6 subscriptions

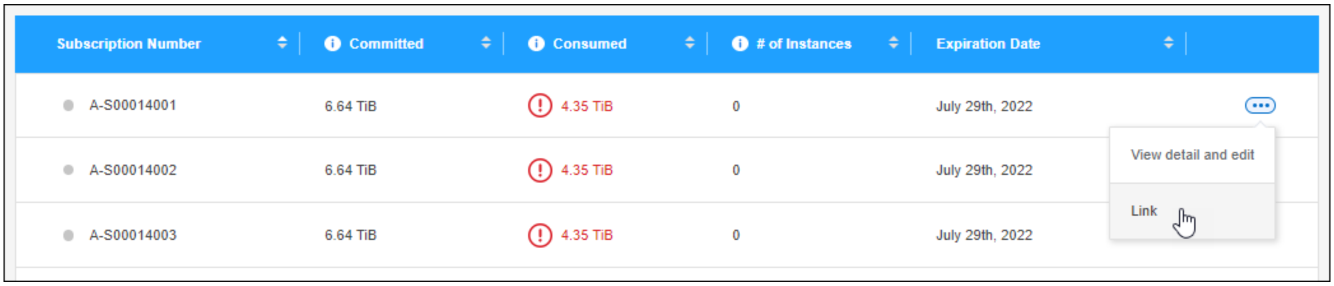
Subscription Number	Committed	Consumed	# of Instances	Expiration Date	
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022	•••
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022	•••
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022	•••
A-S00014004	6.64 TiB	4.35 TiB	0	July 29th, 2022	•••

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**.



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

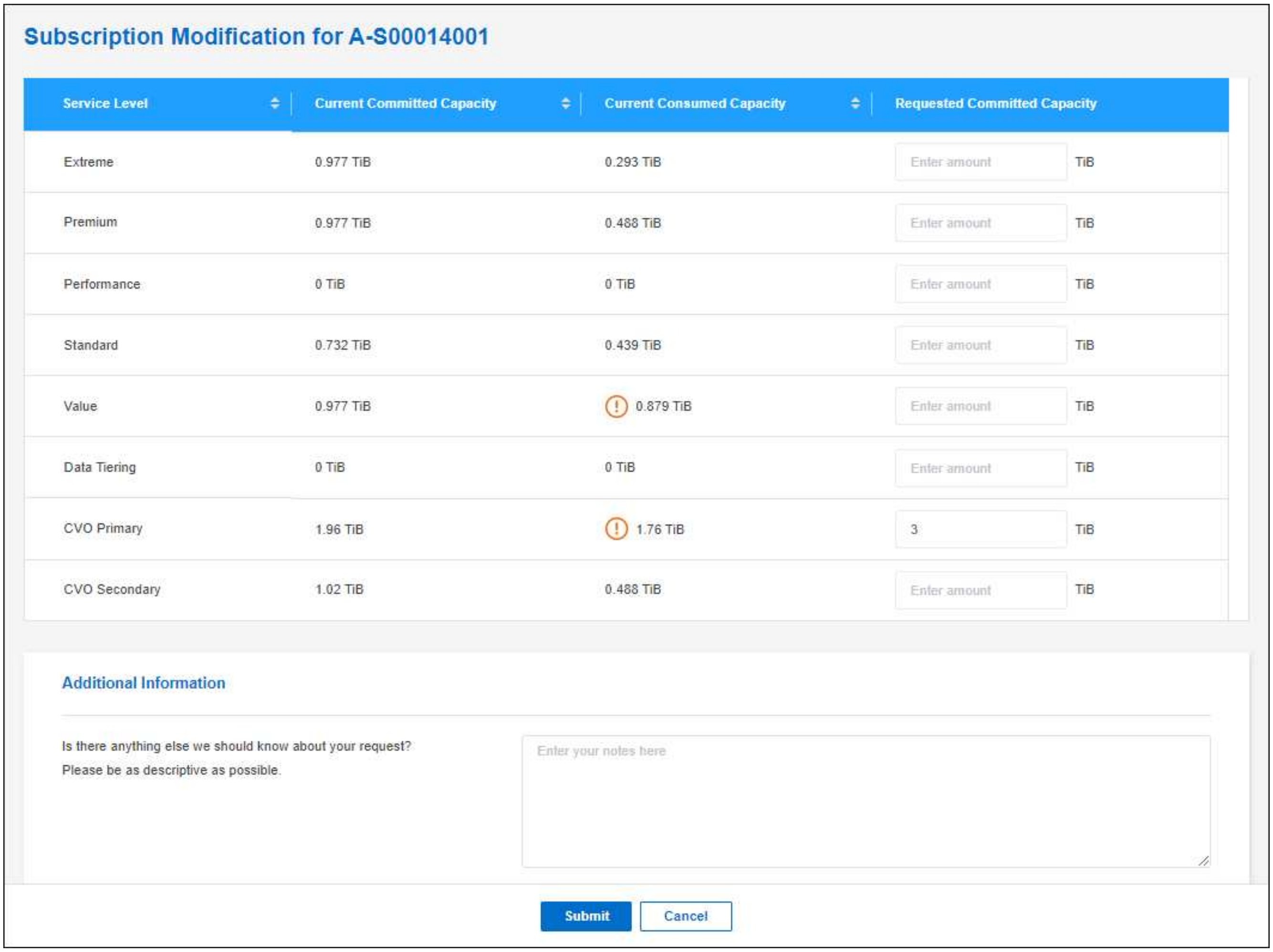
The subscription is now linked to your BlueXP organization or account and available to select when creating a Cloud Volumes ONTAP working environment.

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	Enter amount TiB
Premium	0.977 TiB	0.488 TiB	Enter amount TiB
Performance	0 TiB	0 TiB	Enter amount TiB
Standard	0.732 TiB	0.439 TiB	Enter amount TiB
Value	0.977 TiB	⚠ 0.879 TiB	Enter amount TiB
Data Tiering	0 TiB	0 TiB	Enter amount TiB
CVO Primary	1.96 TiB	⚠ 1.76 TiB	3 TiB
CVO Secondary	1.02 TiB	0.488 TiB	Enter amount TiB

Additional Information

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

Enter your notes here

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.

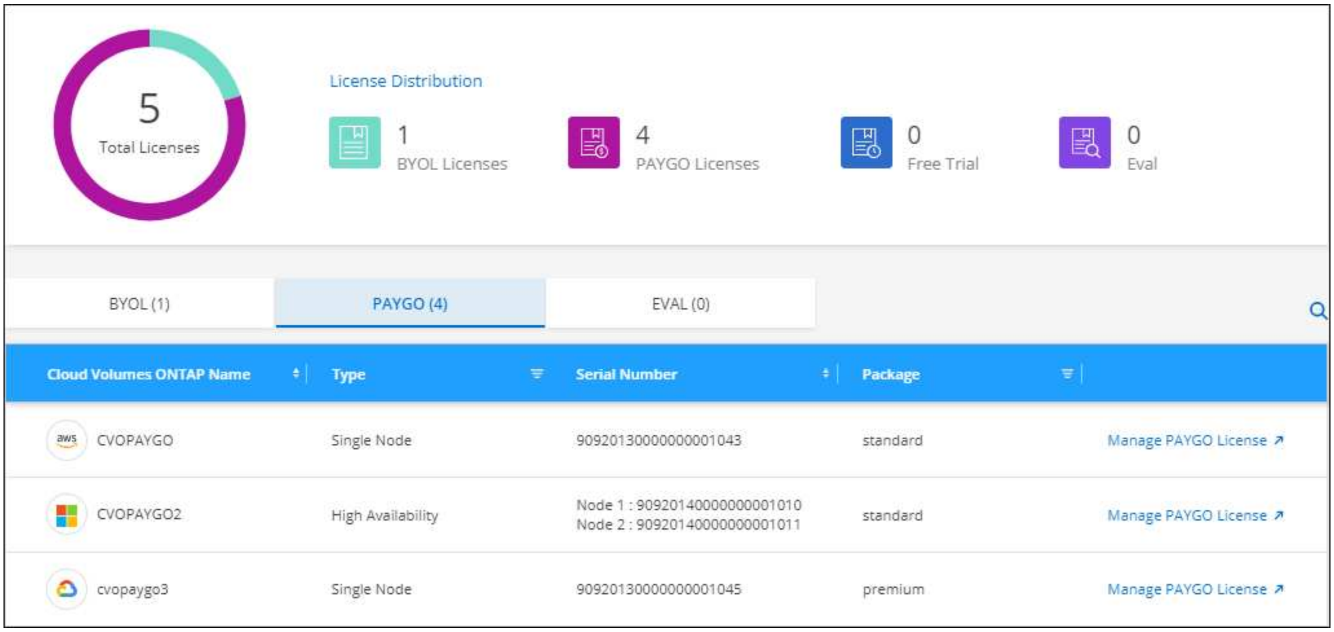
Learn more about Cloud Volumes ONTAP licenses.

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.



Cloud Volumes ONTAP Name	Type	Serial Number	Package	
CVOPAYGO	Single Node	909201300000000001043	standard	Manage PAYGO License ↗
CVOPAYGO2	High Availability	Node 1 : 909201400000000001010 Node 2 : 909201400000000001011	standard	Manage PAYGO License ↗
cvopaygo3	Single Node	909201300000000001045	premium	Manage PAYGO License ↗

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:

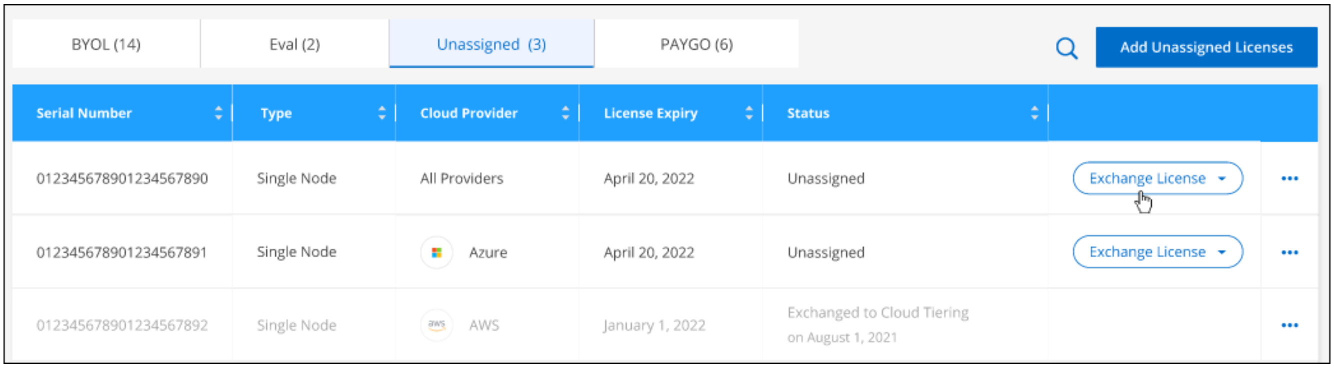
- Licensing for a Cloud Volumes ONTAP HA pair is converted to a 51 TiB direct license
- Licensing for a Cloud Volumes ONTAP single node is converted to a 32 TiB direct license

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**.



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.

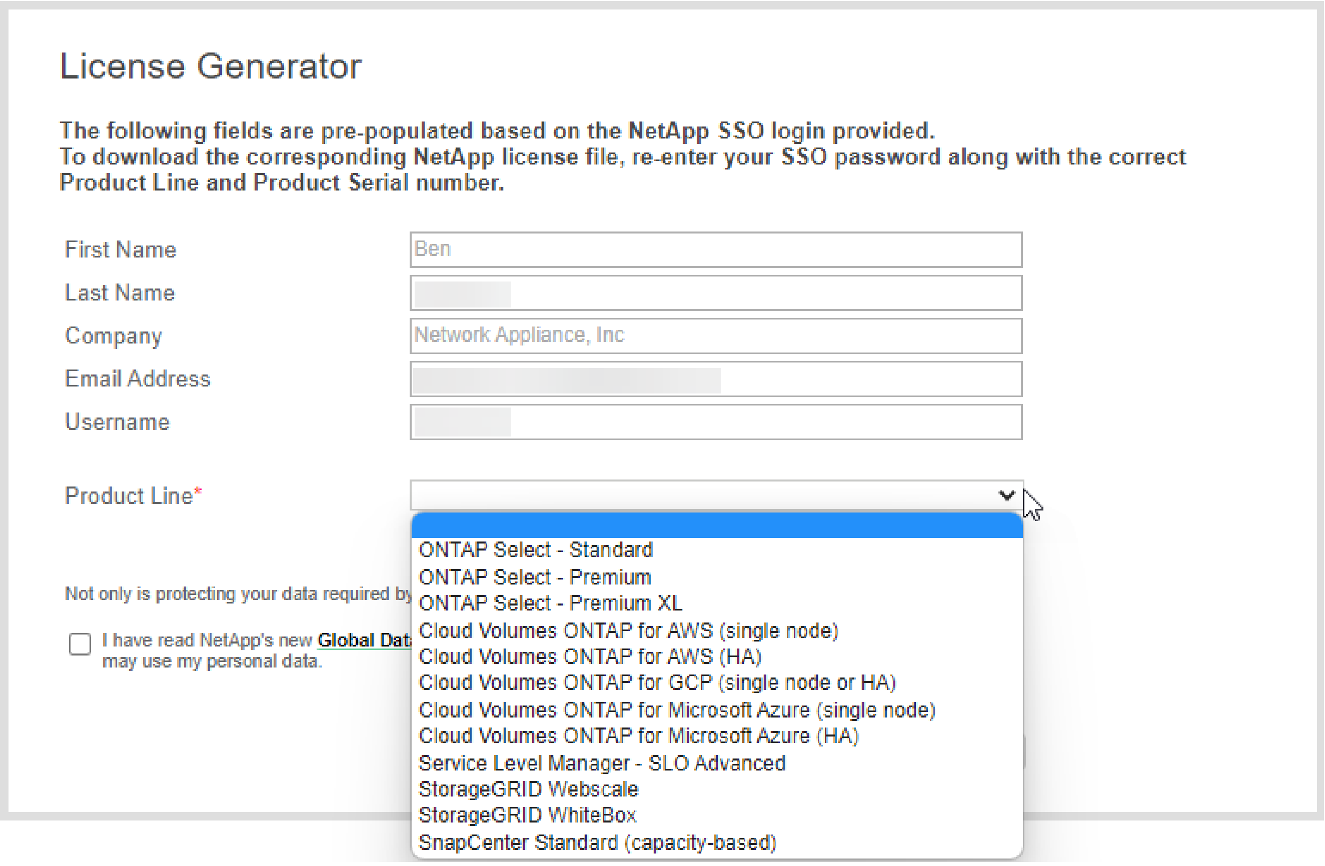
Obtain a system license file

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	[redacted]
Company	Network Appliance, Inc
Email Address	[redacted]
Username	[redacted]
Product Line*	

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)

Not only is protecting your data required by

□ I have read NetApp's new **Global Dat**
may use my personal data.

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

<a href="https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/<a href="concept-licensing.html#end-of-availability-of-node-based-licenses">End of availability of node-based licenses</a><br> xref:./task-convert-node-capacity.html">Convert node-based licenses to capacity based</a>

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.
- If you want to use CIFS in AWS, you must have set up DNS and Active Directory. For details, refer to Networking requirements for Cloud Volumes ONTAP for AWS.
- If your Cloud Volumes ONTAP configuration supports the Amazon EBS Elastic Volumes feature, you might want to learn more about what happens when you create a volume.

Create a volume

The most common way to create a volume is to specify the type of volume that you need and then 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.

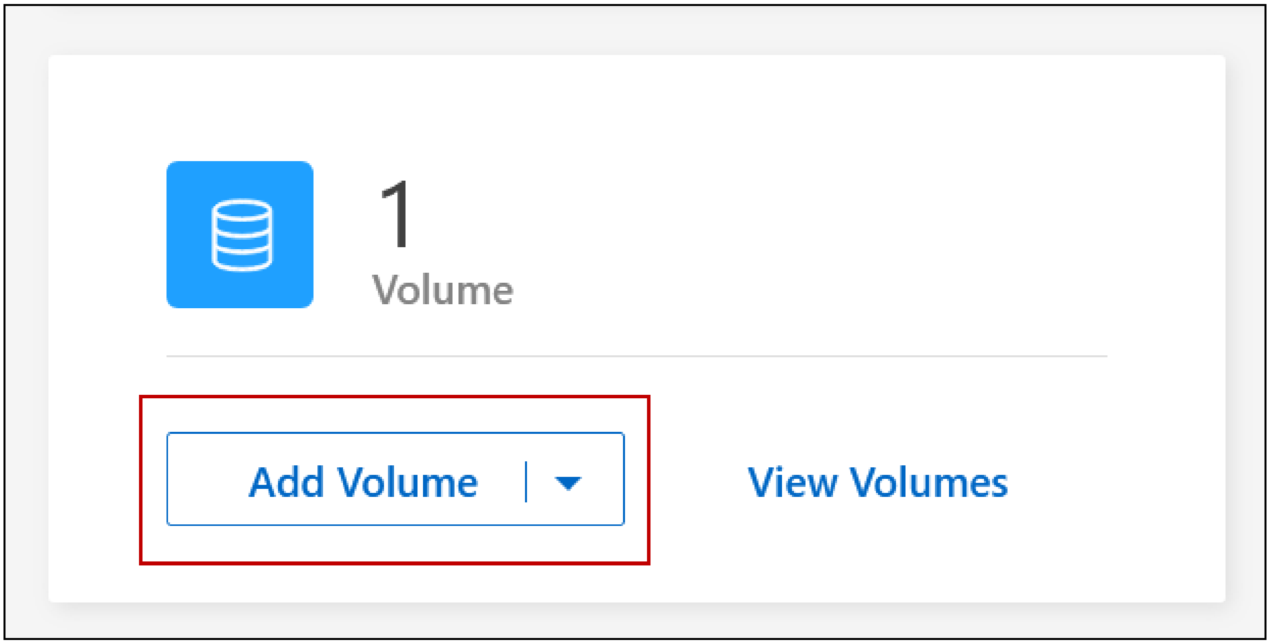
Steps

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.

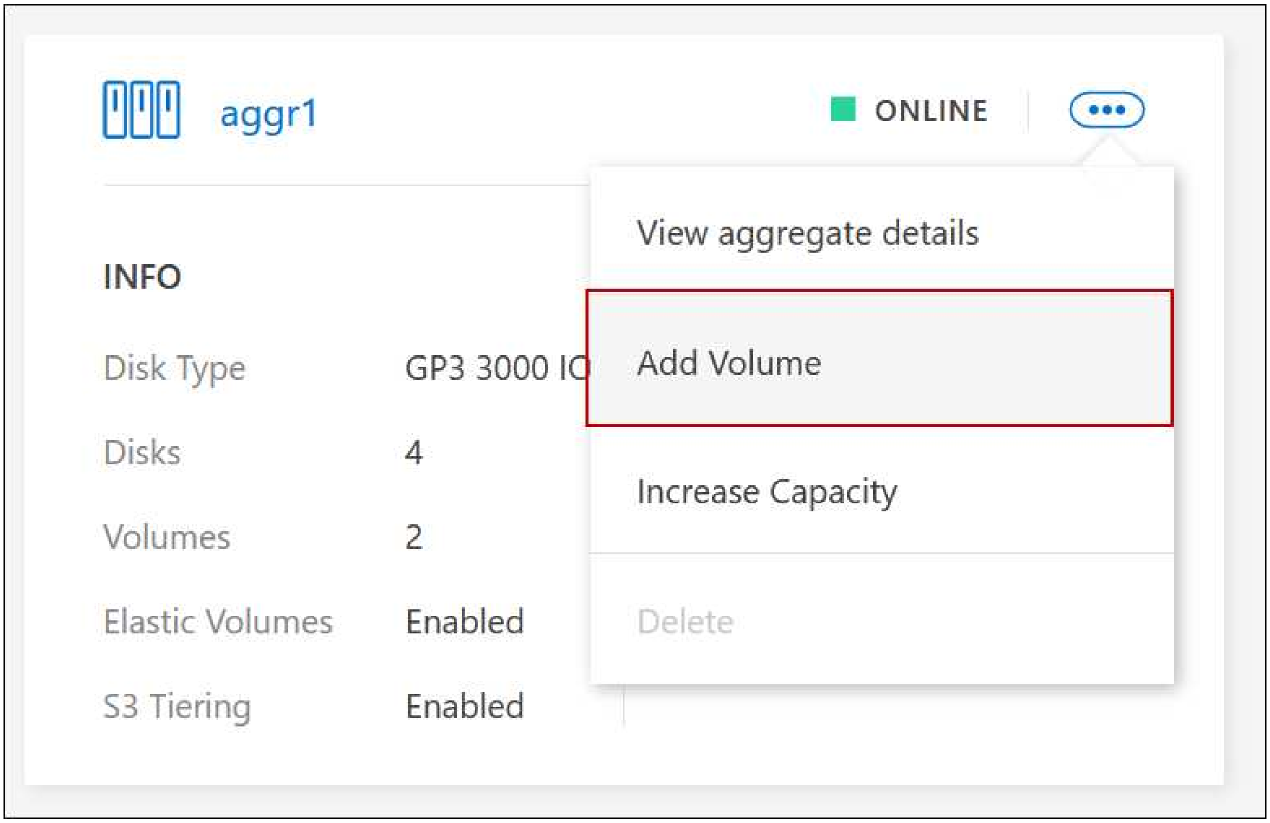
Any aggregate

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.

If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.

Active Directory Domain to join

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

Credentials authorized to join the domain

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

CIFS server NetBIOS name

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

Organizational Unit

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

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

DNS Domain

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

NTP Server

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

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

   - Sizing your system in AWS
   - Sizing your system in Azure
   - Sizing your system in Google Cloud

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

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

   Thin provisioning

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

   Deduplication

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

   Compression

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

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

Result

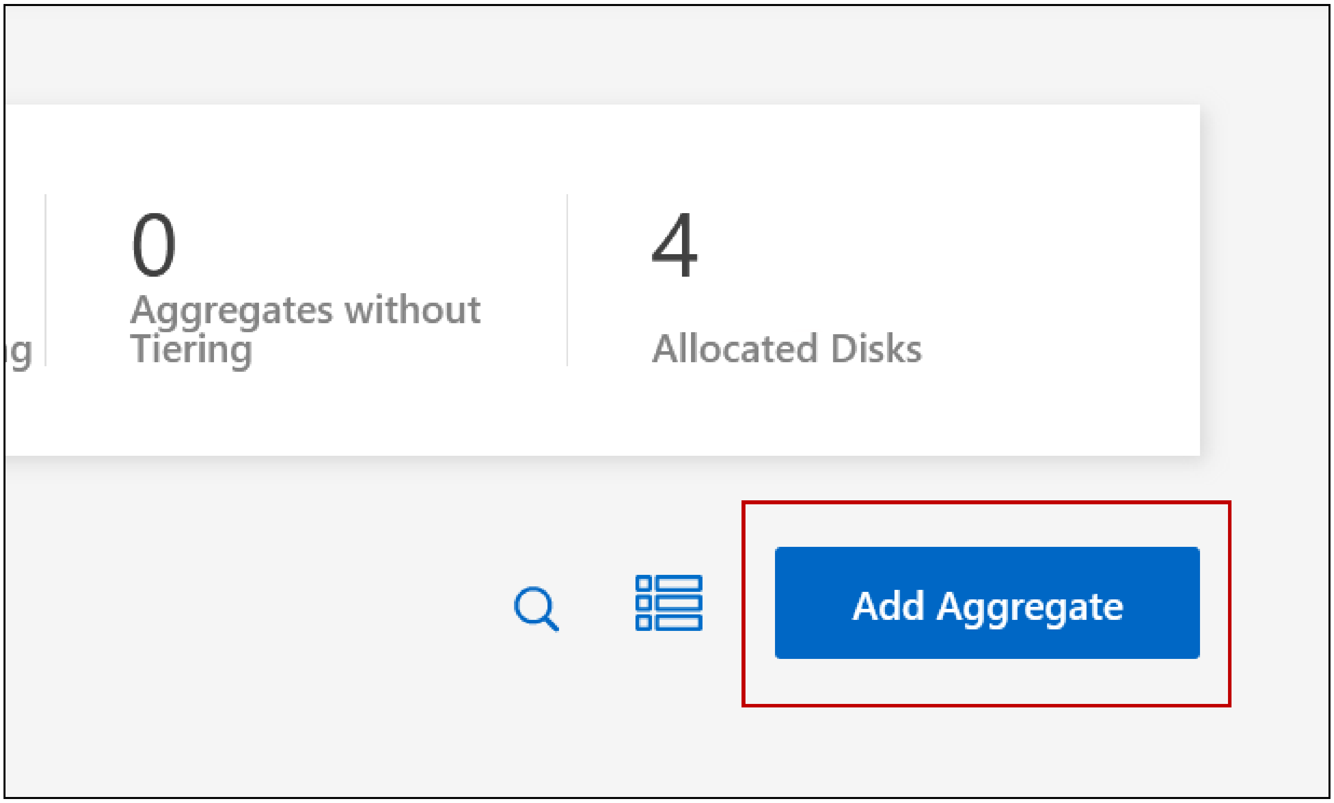
BlueXP creates the volume on the Cloud Volumes ONTAP system.

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.

For HA pairs deployed in multiple AWS Availability Zones, you must mount the volume to clients by using the floating IP address of the node on which the volume resides.

After you create a volume

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

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

Manage volumes on Cloud Volumes ONTAP systems

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

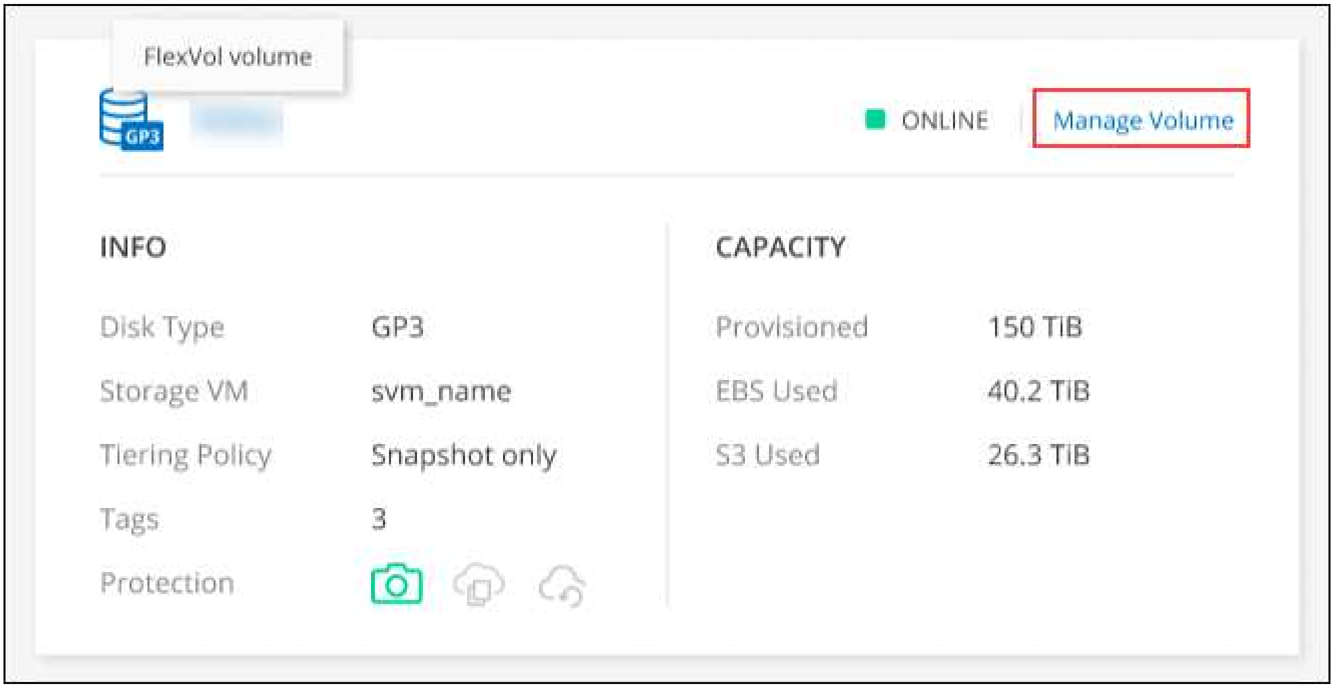
You can manage volumes in BlueXP Standard View or through ONTAP System Manager that is included within BlueXP for advanced volume management. The Standard View provides a limited set of options to modify your volumes. System Manager provides advanced level of management, such as cloning, resizing, changing 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.



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

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	a. Under Volume Actions in the Manage volumes panel, click **Mount Command**. b. Click **Copy**.
Clone a volume	a. Under Volume Actions in the Manage volumes panel, click **Clone the volume**. b. Modify the clone name as needed, and then click **Clone**. This process creates a FlexClone volume. A FlexClone volume is a writable, point-in-time copy that is space-efficient because it uses a small amount of space for metadata, and then only consumes additional space as data is changed or added. To learn more about FlexClone volumes, refer to the ONTAP 9 Logical Storage Management Guide.
Edit a volume (read-write volumes only)	a. Under Volume Actions in the Manage volumes panel, click **Edit volume settings** b. Modify the volume's Snapshot policy, NFS protocol version, NFS access control list (export policy), or share permissions, and then click **Apply**. ⓘ If you need custom Snapshot policies, you can create them by using ONTAP System Manager.
Delete a volume	a. Under Volume Actions in the Manage volumes panel, click **Delete the volume**. b. Under the Delete Volume window, enter the name of the volume you want to delete. c. Click **Delete** again to confirm.
Create a Snapshot copy on demand	a. Under Protection Actions in the Manage Volumes panel, click **Create a Snapshot copy**. b. Change the name, if needed, and then click **Create**.
Restore data from a Snapshot copy to a new volume	a. Under Protection Actions in the Manage Volumes panel, click **Restore from Snapshot copy**. b. Select a Snapshot copy, enter a name for the new volume, and then click **Restore**.

Task	Action
Change the underlying disk type	a. Under Advanced Actions in the Manage Volumes panel, click **Change Disk Type**. b. Select the disk type, and then click **Change**. ⓘ BlueXP moves the volume to an existing aggregate that uses the selected disk type or it creates a new aggregate for the volume.
Change the tiering policy	a. Under Advanced Actions in the Manage Volumes panel, click **Change Tiering Policy**. b. Select a different policy and click **Change**. ⓘ 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.
Delete a volume	a. Select a volume, and then click **Delete**. b. Type the name of the volume in the dialog. c. Click **Delete** again to confirm.

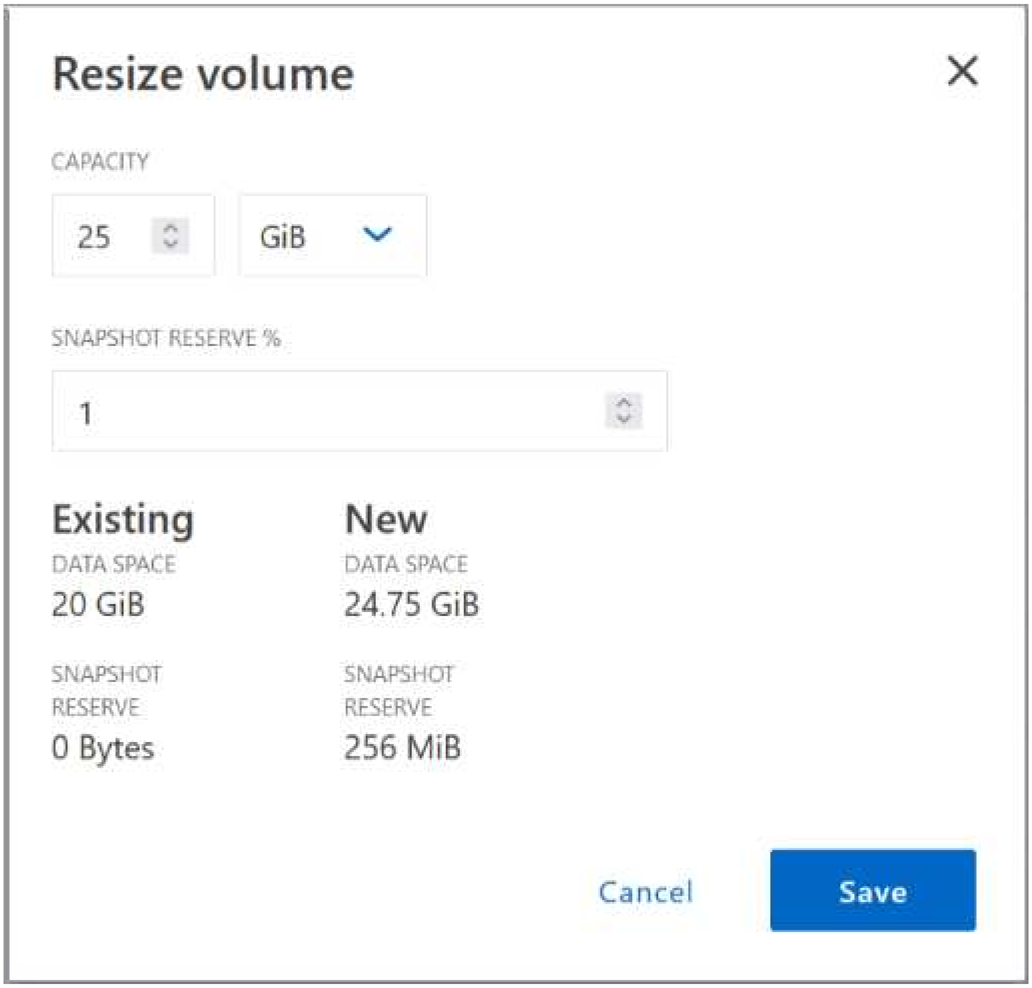
Resize a volume

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

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

Steps

1. Click the System Manager view to resize a volume through ONTAP System Manager. Refer to How to get started.
2. From the left navigation menu, select **Storage > Volumes**.
3. From the list of volumes, identify the one that you should resize.
4. Click the options icon ⋮.
5. Select **Resize**.
6. On the **Resize Volume** screen, edit the capacity and Snapshot reserve percentage as required. You can compare the existing, available space with the modified capacity.
7. Click **Save**.



Resize volume

CAPACITY

25 GiB

SNAPSHOT RESERVE %

1

Existing

DATA SPACE

20 GiB

SNAPSHOT RESERVE

0 Bytes

New

DATA SPACE

24.75 GiB

SNAPSHOT RESERVE

256 MiB

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	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join. If you're configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. • To configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=corp** in this field. • To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, enter **OU=AADDC Computers** or **OU=AADDC Users** in this field. Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain • To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter **OU=Computers,OU=Cloud** in this field. Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD

4. Click **Set**.

Result

Cloud Volumes ONTAP updates the CIFS server with the changes.

Move a volume

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

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

Steps

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

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

   For instructions, refer to the ONTAP 9 Volume Move Express Guide.

Move a volume when 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.

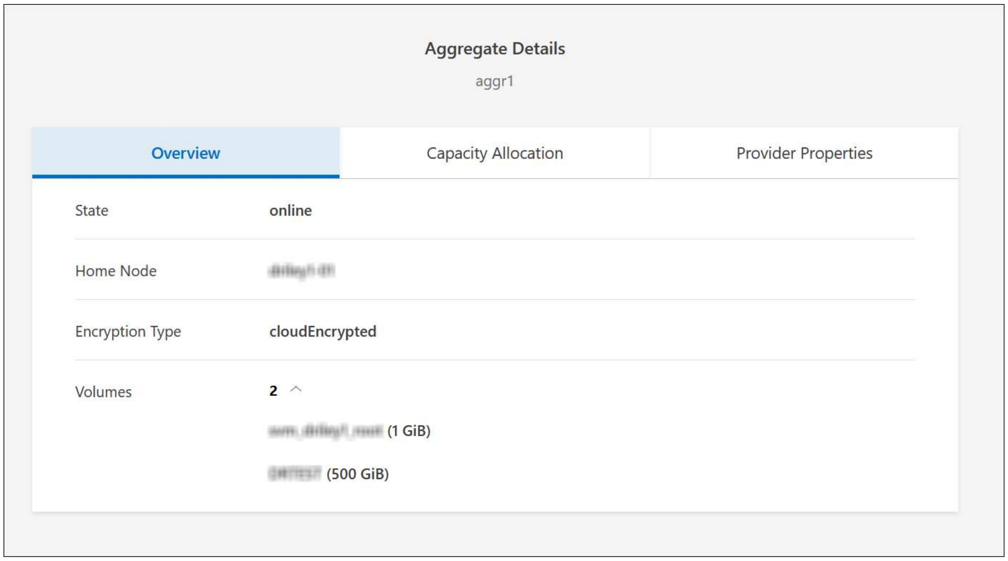
Steps

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.



Aggregate Details

aggr1

State	online
Home Node	[redacted]
Encryption Type	cloudEncrypted
Volumes	2 [redacted] (1 GiB) [redacted] (500 GiB)

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.

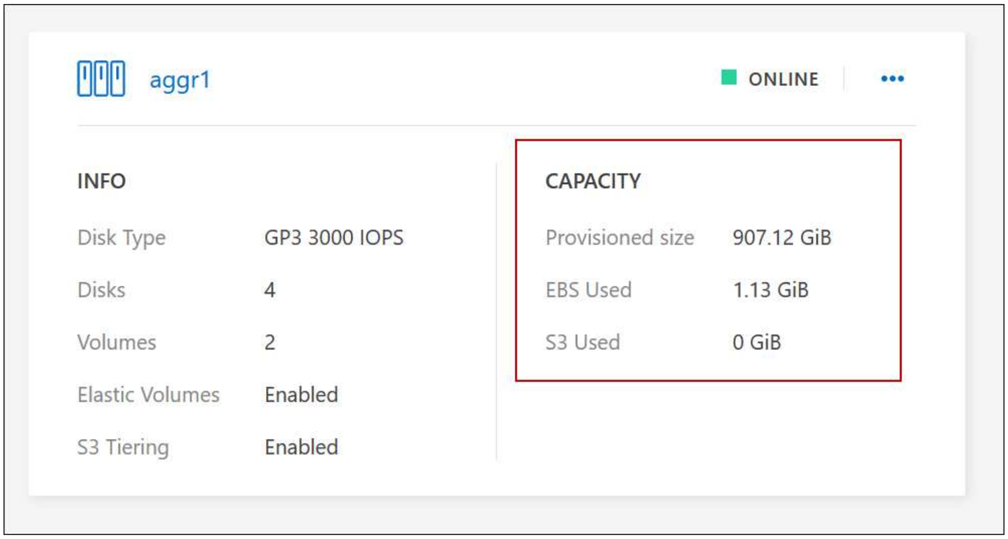
About this task

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).



INFO

Disk Type	GP3 3000 IOPS
Disks	4
Volumes	2
Elastic Volumes	Enabled
S3 Tiering	Enabled

CAPACITY

Provisioned size	907.12 GiB
EBS Used	1.13 GiB
S3 Used	0 GiB

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

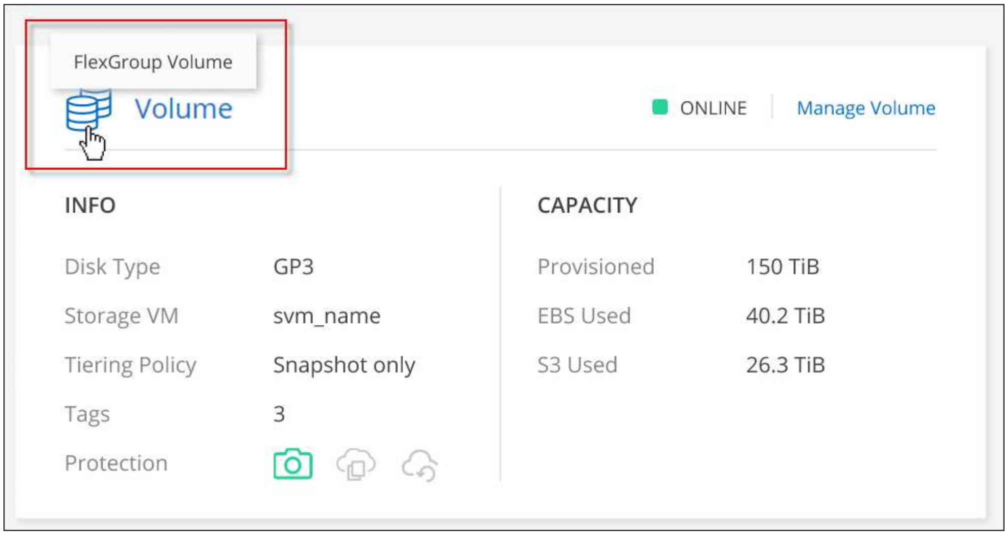
Moving a volume might take longer than you expect if any of the following conditions are true for Cloud Volumes ONTAP:

- 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 FleGroup 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.



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

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 AWS, you'll need a VPC Endpoint to S3. Learn more.
- For Azure, you won't need to do anything as long as BlueXP has the required permissions. Learn more.
- For Google Cloud, you need to configure the subnet for Private Google Access and set up a service account. Learn more.

3 Ensure that you have an aggregate with tiering enabled

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

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

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 AWS

- Data tiering is supported in AWS beginning with Cloud Volumes ONTAP 9.2.
- The performance tier can be General Purpose SSDs (gp3 or gp2) or Provisioned IOPS SSDs (io1).

> ⓘ We do not recommend tiering data to object storage when using Throughput Optimized HDDs (st1).

- The inactive data is tiered to Amazon S3 buckets. Tiering to other providers is not supported.

Support in Azure

- Data tiering is supported in Azure as follows:
  - Version 9.4 in with single node systems
  - Version 9.6 in with HA pairs
- The performance tier can be Premium SSD managed disks, Standard SSD managed disks, or Standard HDD managed disks.
- The inactive data is tiered to Microsoft Azure Blob. Tiering to other providers is not supported.

Support in Google Cloud

- Data tiering is supported in Google Cloud beginning with Cloud Volumes ONTAP 9.6.
- The performance tier can be either SSD persistent disks, balanced persistent disks, or standard persistent disks.
- The inactive data is tiered to Google Cloud Storage. Tiering to other providers is not supported.

Feature interoperability

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

Requirements

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

Requirements to tier cold data to AWS S3

Ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, refer to the AWS Documentation: Creating a Gateway Endpoint.

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

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

Requirements to tier cold data to Azure Blob storage

You don't need to set up a connection between the performance tier and the capacity tier as long as 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

Requirements to tier cold data to a Google Cloud Storage bucket

- The subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access. For instructions, refer to Google Cloud Documentation: Configuring Private Google Access.
- A service account must be attached to Cloud Volumes ONTAP.

  Learn how to set up this service account.

  You're prompted to select this service account when you create a Cloud Volumes ONTAP working environment.

  If you don't select a service account during deployment, you'll need to shut down Cloud Volumes ONTAP, go to the Google Cloud console, and then attach the service account to the Cloud Volumes ONTAP instances. You can then enable data tiering as described in the next section.

- To encrypt the bucket with customer-managed encryption keys, enable the Google Cloud storage bucket to use the key.

  Learn how to use customer-managed encryption keys with Cloud Volumes ONTAP.

Enable data tiering after implementing the requirements

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**

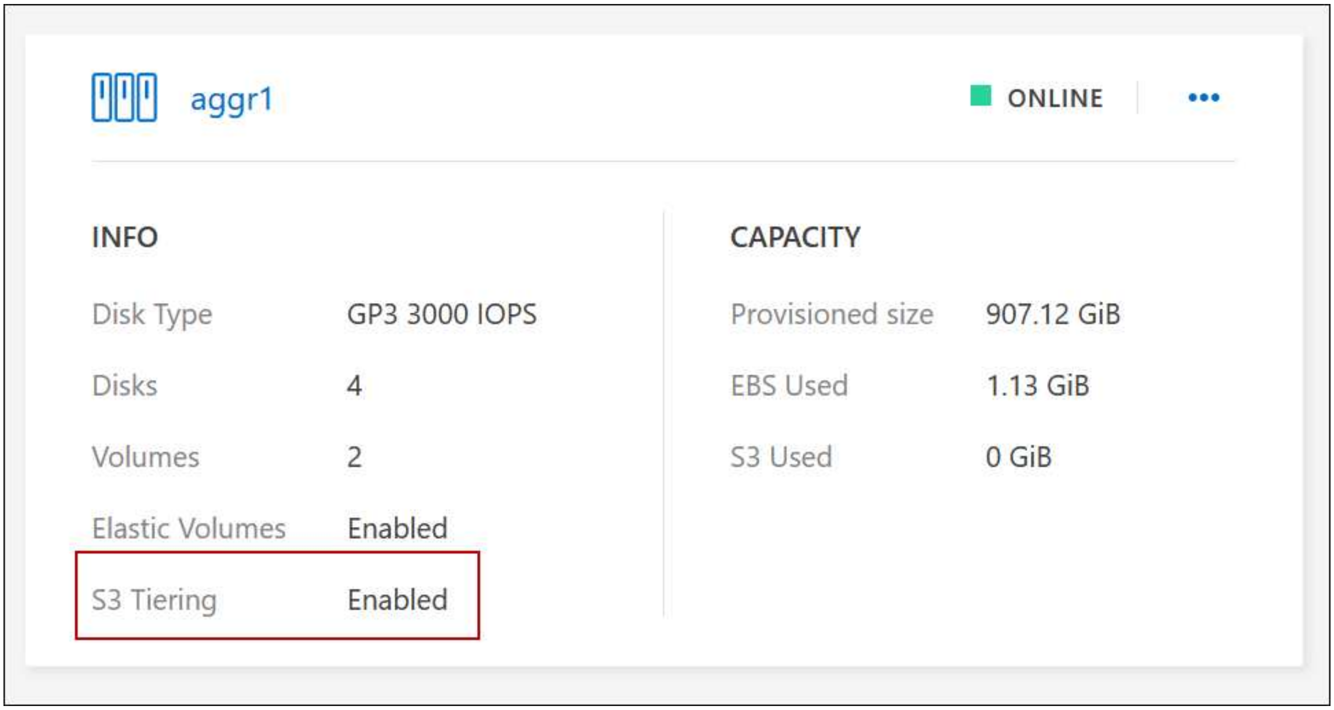
  If you're enabling data tiering on a new volume, then you don't need to worry about enabling data tiering on an aggregate. BlueXP creates the volume on an existing aggregate that has tiering enabled, or it creates a new aggregate for the volume if a data tiering-enabled aggregate doesn't already exist.

- **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.



aggr1

🟩 ONLINE

INFO

Disk Type GP3 3000 IOPS

Disks 4

Volumes 2

Elastic Volumes Enabled

S3 Tiering Enabled

CAPACITY

Provisioned size 907.12 GiB

EBS Used 1.13 GiB

S3 Used 0 GiB

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

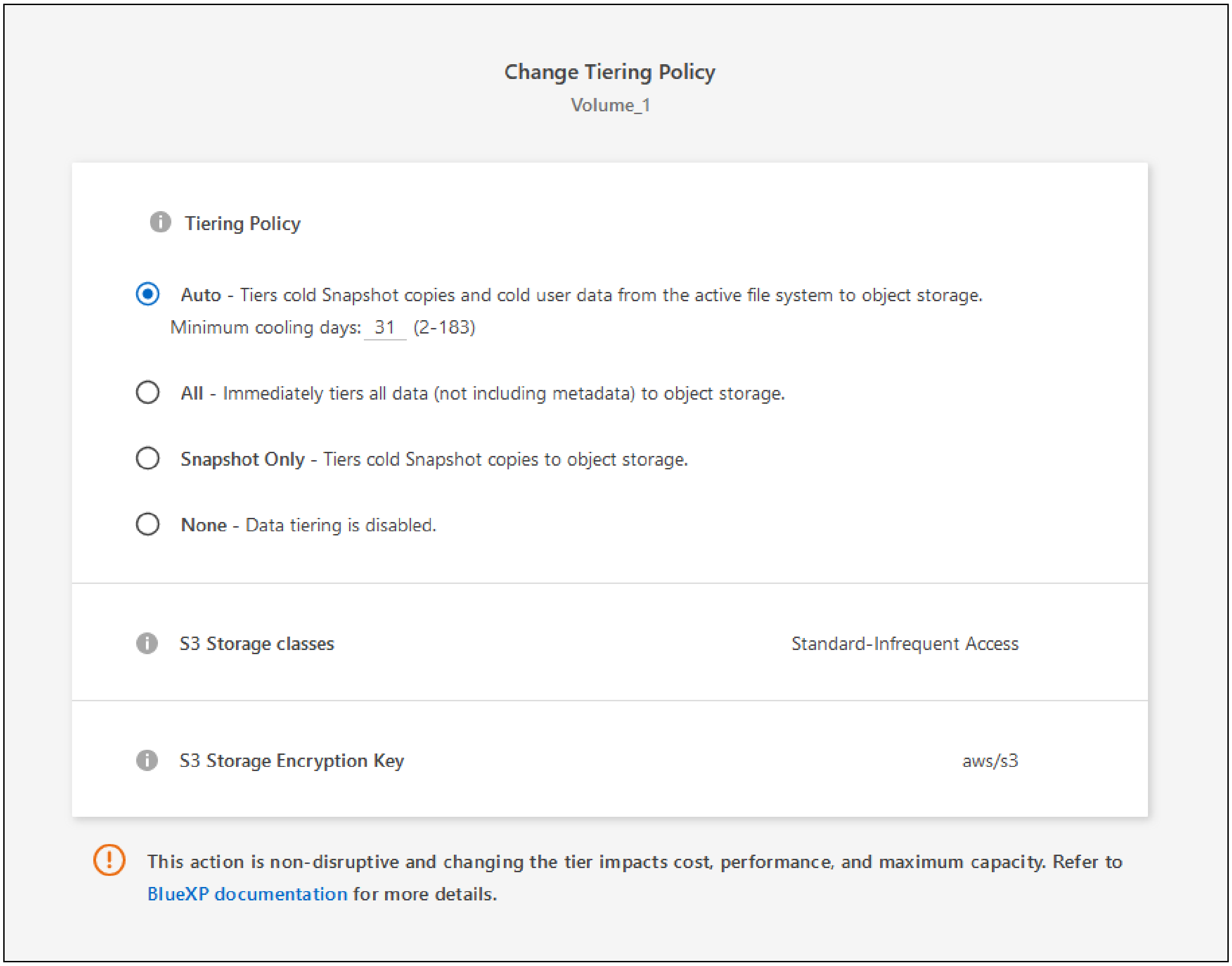
1. In Volumes tab under the working environment, create a new volume or change the tier of an existing volume:

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

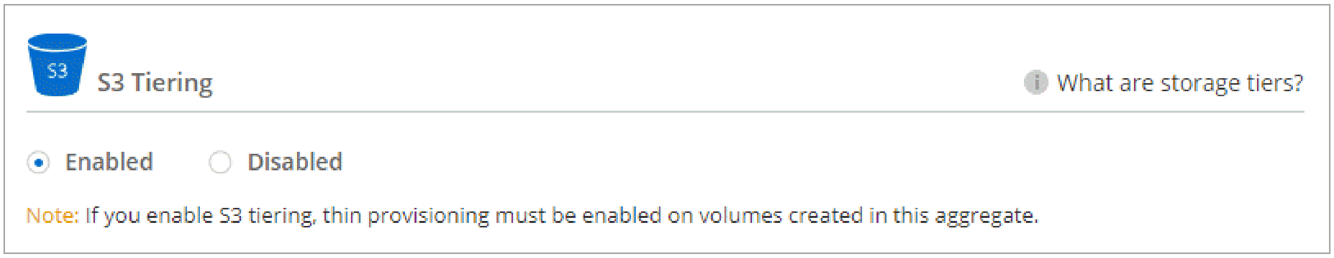
Cloud Volumes ONTAP can tier data from a data protection volume to a capacity tier. If you activate the destination volume, the data gradually moves to the performance tier as it is read.

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

   ● 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).

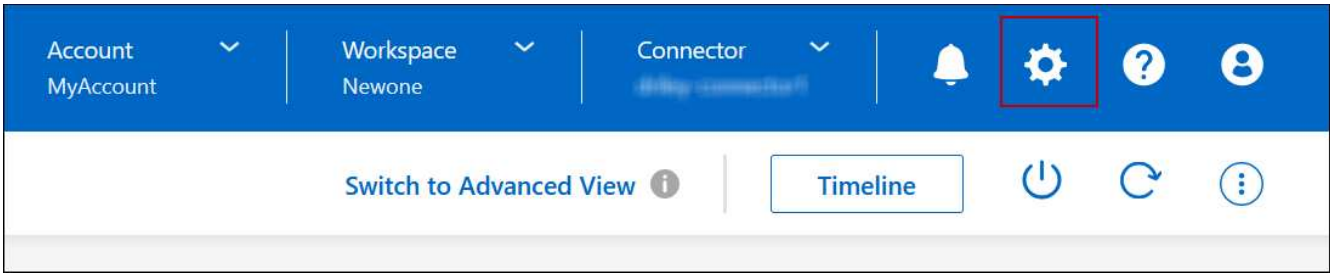
> If there isn't sufficient space, then Cloud Volumes ONTAP can't move the data and you might experience performance degradation. Any change should be done with caution. If you're unsure, reach out to NetApp Support for guidance.

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: vserver 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

Cloud Volumes ONTAP
FlexCache with Cloud Volumes ONTAP
Technical Demo
Chris Hurley
Technical Marketing Engineer

Work with FlexCache when the origin is encrypted

When configuring FlexCache on a Cloud Volumes ONTAP system where the origin volume is encrypted, additional steps are required, to ensure that the FlexCache volume can properly access and cache the encrypted data.

Before you begin

1. **Encryption setup**: Ensure that the source volume is fully encrypted and operational. For Cloud Volumes ONTAP systems, this involves integrating with cloud-specific key management services.
For AWS, this typically means using AWS Key Management Service (KMS). For information, refer to Manage keys with AWS Key Management Service.
For Azure, you need to set up Azure Key Vault for NetApp Volume Encryption (NVE). For information, refer to Manage keys with Azure Key Vault.
For Google Cloud, it is Google Cloud Key Management Service. For information, refer to Manage keys with Google's Cloud Key Management Service.
2. **Key management services**: Before creating a FlexCache volume, verify that the key management services are configured correctly on the Cloud Volumes ONTAP system. This configuration is essential for the FlexCache volume to decrypt the data from the origin volume.
3. **Licensing**: Confirm that a valid FlexCache license is available and activated on the Cloud Volumes ONTAP system.
4. **ONTAP version**: Ensure that the ONTAP version of your Cloud Volumes ONTAP system supports FlexCache with encrypted volumes. Refer to the latest ONTAP release notes or compatibility matrix for more information.
5. **Network Configuration**: Ensure that the network configuration allows for seamless communication between the origin volume and the FlexCache volume. This includes proper routing and DNS resolution in a cloud environment.

Steps

Create a FlexCache volume on your Cloud Volumes ONTAP system with an encrypted source volume. For detailed steps and additional considerations, refer to the following sections:

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

Aggregate administration

Create an aggregate for Cloud Volumes ONTAP systems

You can create aggregates yourself or let 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.

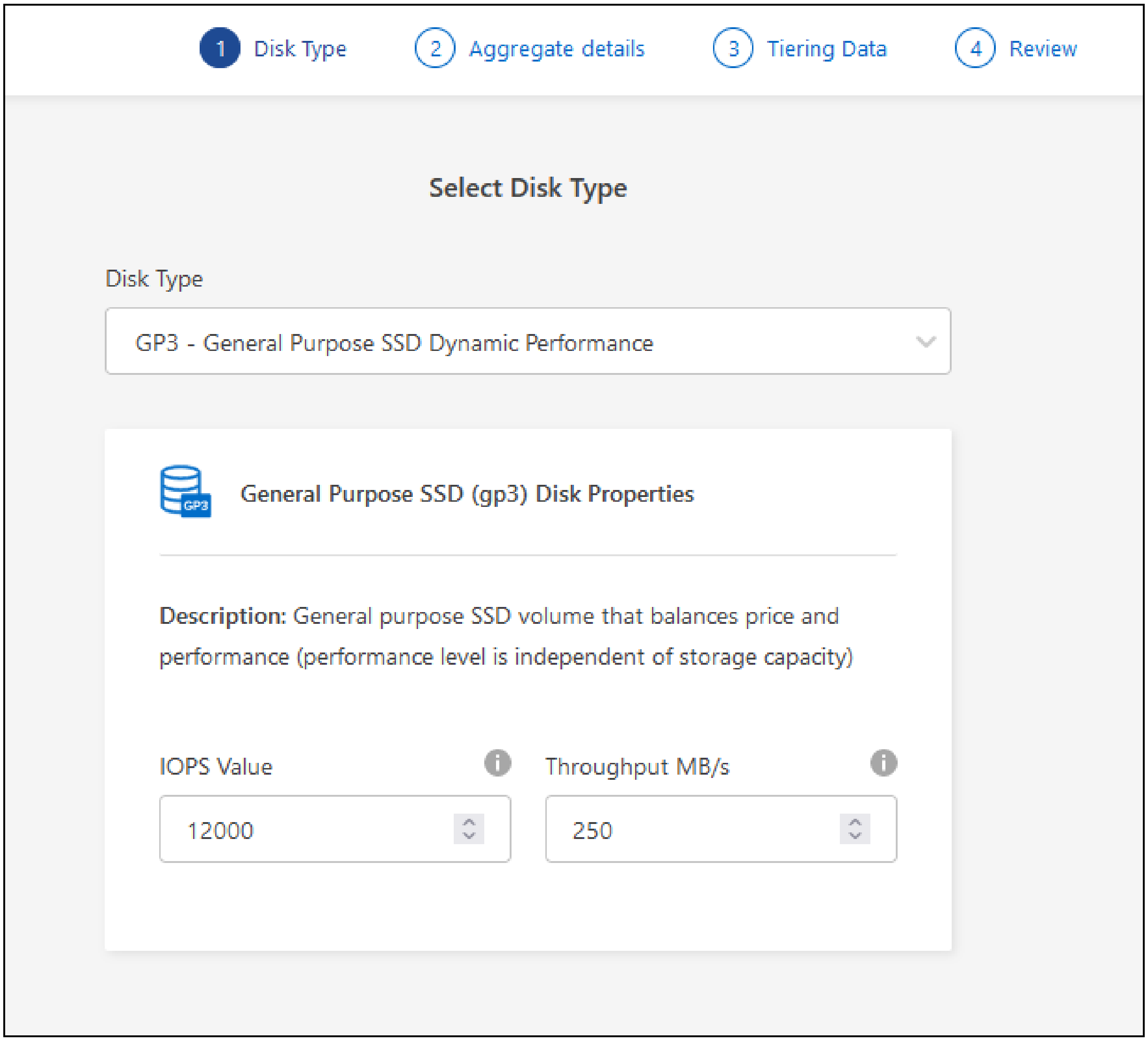
> ⚠ All disks and aggregates must be created and deleted directly from BlueXP. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

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.

AWS

- If you’re prompted to choose a disk type and disk size, refer to Plan your Cloud Volumes ONTAP configuration in AWS.
- If you’re prompted to enter the aggregate’s capacity size, then you’re creating an aggregate on a configuration that supports the Amazon EBS Elastic Volumes feature. The following screenshot shows an example of a new aggregate comprised of gp3 disks.



Select Disk Type

Disk Type: GP3 - General Purpose SSD Dynamic Performance

General Purpose SSD (gp3) Disk Properties

Description: General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)

IOPS Value: 12000

Throughput MB/s: 250

Learn more about support for Elastic Volumes.

Azure

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

Google Cloud

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

4. Click **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

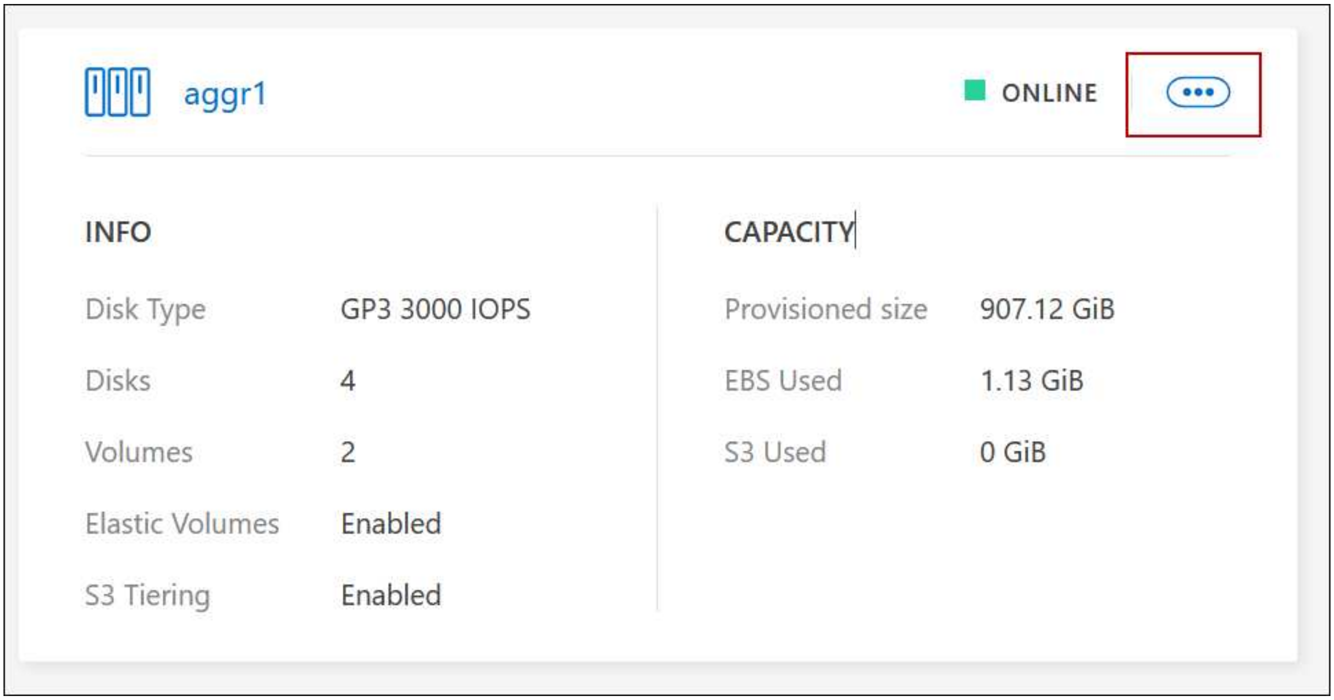
If you want to delete an aggregate, you must have first deleted the volumes in the aggregate.

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)**.



aggr1 🟩 ONLINE •••

INFO

Disk Type	GP3 3000 IOPS
Disks	4
Volumes	2
Elastic Volumes	Enabled
S3 Tiering	Enabled

CAPACITY

Provisioned size	907.12 GiB
EBS Used	1.13 GiB
S3 Used	0 GiB

5. Manage your aggregates:

Task	Action
View information about an aggregate	Under the … (ellipses icon) menu, click **View aggregate details**.

Task	Action
Create a volume on a specific aggregate	Under the … (ellipses icon) menu, click **Add volume**.
Add disks to an aggregate	a. Under the … (ellipses icon) menu, click **Add disks**. b. Select the number of disks that you want to add and click **Add**. All disks in an aggregate must be the same size.
Increase the capacity of an aggregate that supports Amazon EBS Elastic Volumes	a. Under the … (ellipses icon) menu, click **Increase capacity**. b. Enter the additional capacity that you'd like to add and then click **Increase**. Note that you must increase the capacity of the aggregate by a minimum of 256 GiB or 10% of the aggregate's size. For example, if you have a 1.77 TiB aggregate, 10% is 181 GiB. That's lower than 256 GiB, so the size of the aggregate must in increased by the 256 GiB minimum.
Delete an aggregate	a. Select an aggregate tile that does not contain any volumes click the **… (ellipses icon) > Delete**. b. 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.

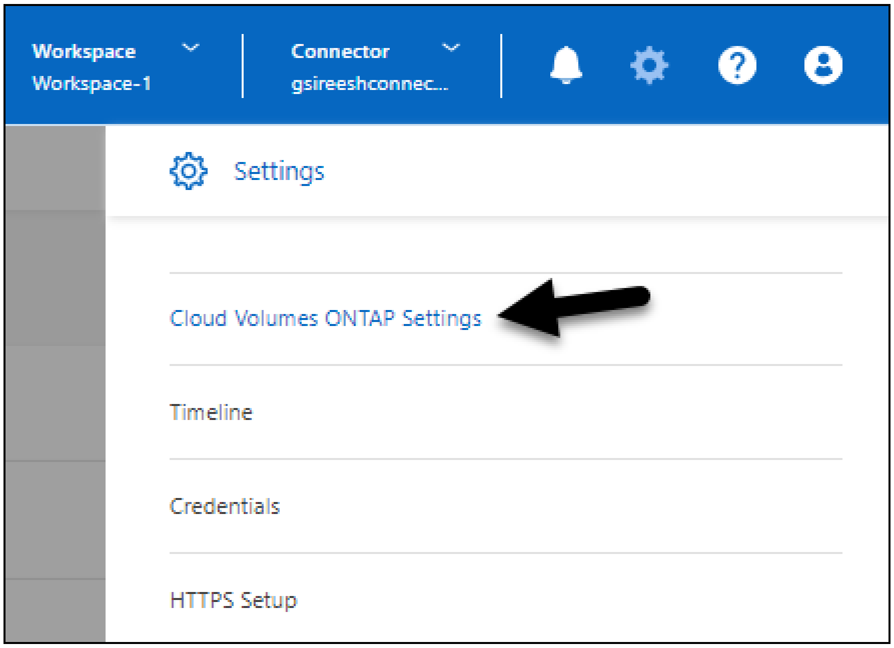
These settings affect all Cloud Volumes ONTAP systems managed by a Connector. If you have another Connector, it can be configured differently.

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

   Refer to Automatic capacity management to learn now capacity is automatically managed in Cloud Volumes ONTAP.

   Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering

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

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

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.

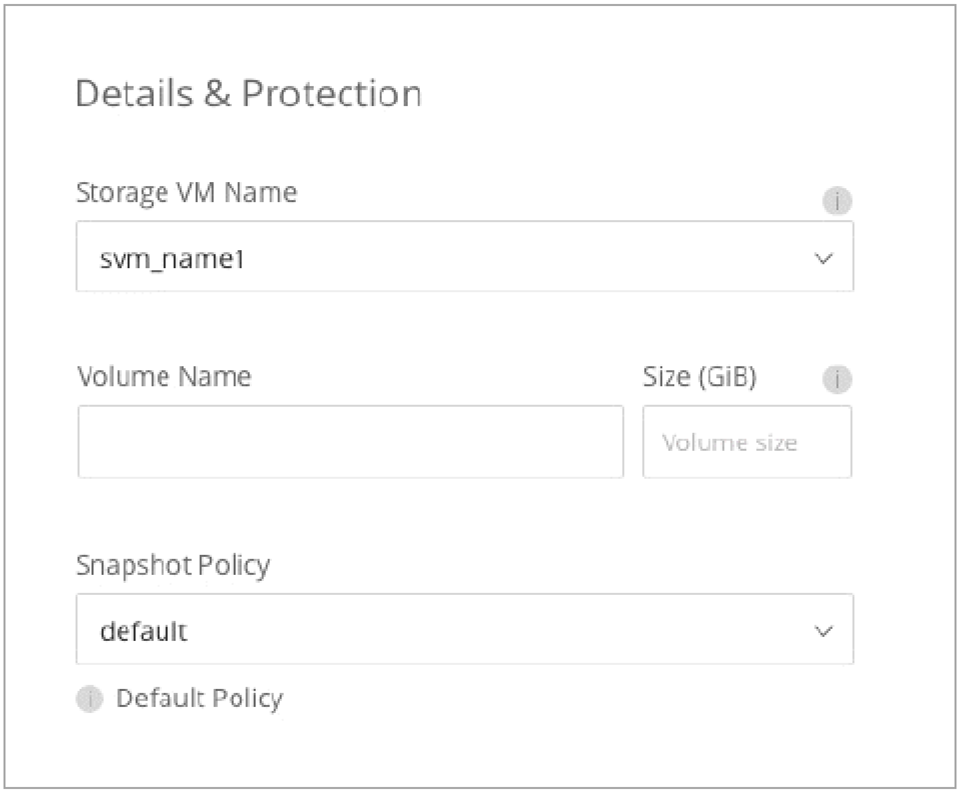
Supported number of storage VMs

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)

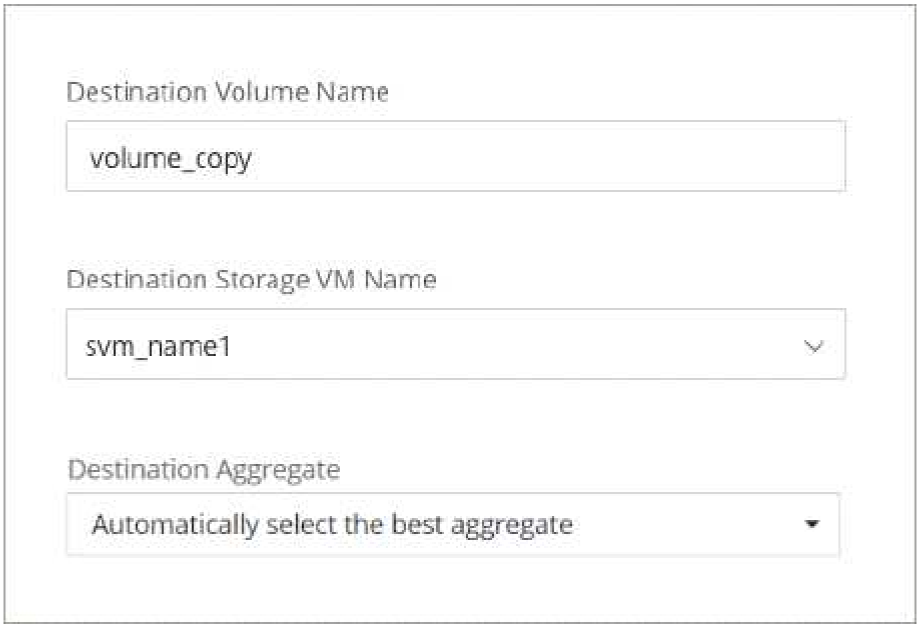
Volume size

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 AWS

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

To create additional data-serving storage VMs, you need to allocate IP addresses in AWS and then run ONTAP commands based on your Cloud Volumes ONTAP configuration.

Supported number of storage VMs

Multiple storage VMs are supported with specific Cloud Volumes ONTAP configurations starting with the 9.7 release. Go to the Cloud Volumes ONTAP Release Notes to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

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

Verify limits for your configuration

Each EC2 instance supports a maximum number of private IPv4 addresses per network interface. You need to verify the limit before you allocate IP addresses in AWS for the new storage VM.

Steps

1. Go the Storage limits section in the Cloud Volumes ONTAP Release Notes.

2. Identify the maximum number of IP addresses per interface for your instance type.
3. Make note of this number because you'll need it in the next section when you allocate IP addresses in AWS.

Allocate IP addresses in AWS

Private IPv4 addresses must be assigned to port e0a in AWS before you create LIFs for the new storage VM.

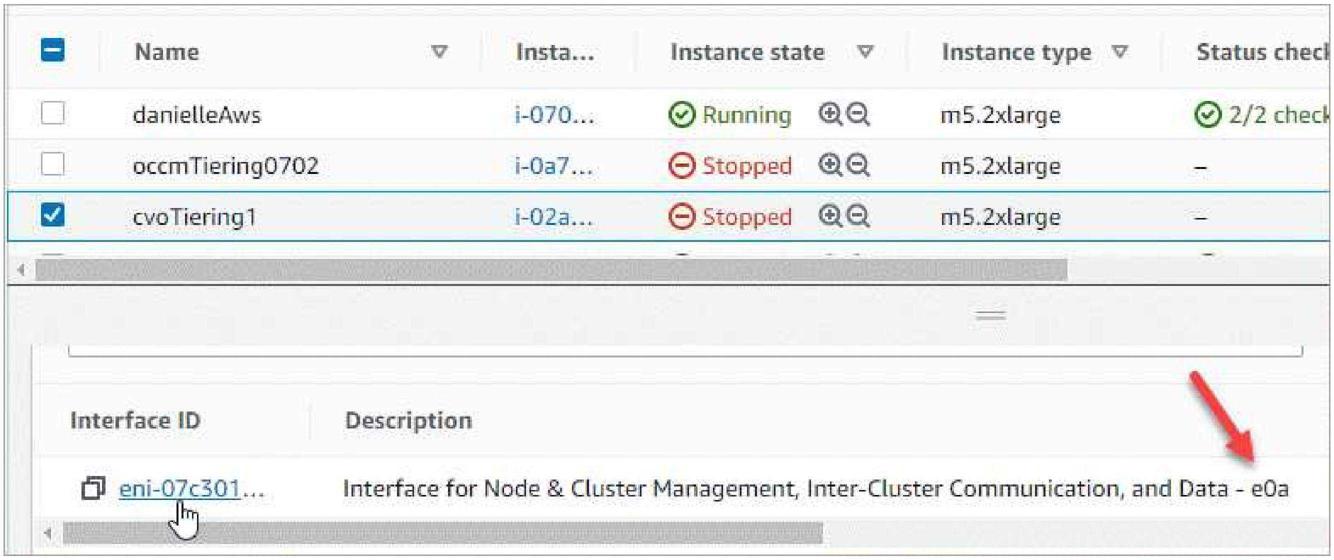
Note that an optional management LIF for a storage VM requires a private IP address on a single node system and on an HA pair in a single AZ. This management LIF provides a connection to management tools like SnapCenter.

Steps

1. Log in to AWS and open the EC2 service.
2. Select the Cloud Volumes ONTAP instance and click **Networking**.

   If you're creating a storage VM on an HA pair, select node 1.

3. Scroll down to **Network interfaces** and click the **Interface ID** for port e0a.



☐	Name	Insta...	Instance state	Instance type	Status checl
☐	danielleAws	i-070...	✓ Running	m5.2xlarge	✓ 2/2 checl
☐	occmTiering0702	i-0a7...	⊖ Stopped	m5.2xlarge	–
☑	cvoTiering1	i-02a...	⊖ Stopped	m5.2xlarge	–

Interface ID	Description
eni-07c301...	Interface for Node & Cluster Management, Inter-Cluster Communication, and Data - e0a

4. Select the network interface and click **Actions > Manage IP addresses**.
5. Expand the list of IP addresses for e0a.
6. Verify the IP addresses:
   a. Count the number of allocated IP addresses to confirm that the port has room for additional IPs.

      You should have identified the maximum number of supported IP addresses per interface in the previous section of this page.

   b. Optional: Go to the ONTAP CLI for Cloud Volumes ONTAP and run **network interface show** to confirm that each of these IP addresses are in use.

      If an IP address isn't in use, then you can use it with the new storage VM.

7. Back in the AWS Console, click **Assign new IP address** to assign additional IP addresses based on the amount that you need for the new storage VM.

- Single node system: One unused secondary private IP is required.

  An optional secondary private IP is required if you want to create a management LIF on the storage VM.

- HA pair in a single AZ: One unused secondary private IP is required on node 1.

  An optional secondary private IP is required if you want to create a management LIF on the storage VM.

- HA pair in multiple AZs: One unused secondary private IP is required on each node.

8. If you’re allocating the IP address on an HA pair in a single AZ, enable **Allow secondary private IPv4 addresses to be reassigned**.
9. Click **Save**.
10. If you have an HA pair in multiple AZs, then you’ll need to repeat these steps for node 2.

Create a storage VM on a single node system

These steps create a new storage VM on a single node system. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

Steps

1. Create the storage VM and a route to the storage VM.

   ```
   vserver create -rootvolume-security-style unix -rootvolume root_svm_2
   -snapshot-policy default -vserver svm_2 -aggregate aggr1
   ```

   ```
   network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
   subnet_gateway
   ```

2. Create a NAS LIF.

   ```
   network interface create -auto-revert true -vserver svm_2 -service
   -policy default-data-files -home-port e0a -address private_ip_x -netmask
   node1Mask -lif ip_nas_2 -home-node cvo-node
   ```

   Where *private_ip_x* is an unused secondary private IP on e0a.

3. Optional: Create a storage VM management LIF.

   ```
   network interface create -auto-revert true -vserver svm_2 -service
   -policy default-management -home-port e0a -address private_ip_y -netmask
   node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
   ```

   Where *private_ip_y* is another unused secondary private IP on e0a.

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

   This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

Create a storage VM on an HA pair in a single AZ

These steps create a new storage VM on an HA pair in a single AZ. One private IP address is required to create a NAS LIF and another optional private IP address is needed if you want to create a management LIF.

Both of these LIFs get allocated on node 1. The private IP addresses can move between nodes if failures occur.

Steps

1. Create the storage VM and a route to the storage VM.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. Create a NAS LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

   Where *private_ip_x* is an unused secondary private IP on e0a of cvo-node1. This IP address can be relocated to the e0a of cvo-node2 in case of takeover because the service policy default-data-files indicates that IPs can migrate to the partner node.

3. Optional: Create a storage VM management LIF on node 1.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

   Where *private_ip_y* is another unused secondary private IP on e0a.

4. Assign one or more aggregates to the storage VM.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

5. If you’re running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

   Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Create a storage VM on an HA pair in multiple AZs

These steps create a new storage VM on an HA pair in multiple AZs.

A *floating* IP address is required for a NAS LIF and is optional for a management LIF. These floating IP addresses don't require you to allocate private IPs in AWS. Instead, the floating IPs are automatically configured in the AWS route table to point to a specific node's ENI in the same VPC.

In order for floating IPs to work with ONTAP, a private IP address must be configured on every storage VM on each node. This is reflected in the steps below where an iSCSI LIF is created on node 1 and on node 2.

Steps

1. Create the storage VM and a route to the storage VM.

   ```
   vserver create -rootvolume-security-style unix -rootvolume root_svm_2
   -snapshot-policy default -vserver svm_2 -aggregate aggr1
   ```

   ```
   network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
   subnet_gateway
   ```

2. Create a NAS LIF on node 1.

   ```
   network interface create -auto-revert true -vserver svm_2 -service
   -policy default-data-files -home-port e0a -address floating_ip -netmask
   node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
   ```

   - The floating IP address must be outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. 192.168.209.27 is an example floating IP address. Learn more about choosing a floating IP address.
   - `-service-policy default-data-files` indicates that IPs can migrate to the partner node.

3. Optional: Create a storage VM management LIF on node 1.

   ```
   network interface create -auto-revert true -vserver svm_2 -service
   -policy default-management -home-port e0a -address floating_ip -netmask
   node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
   ```

4. Create an iSCSI LIF on node 1.

   ```
   network interface create -vserver svm_2 -service-policy default-data-
   blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
   ip_node1_iscsi_2 -home-node cvo-node1
   ```

   - This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn't have to be an iSCSI LIF, but it can't be configured to migrate between nodes.
   - `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.

   - *private_ip* is an unused secondary private IP address on eth0 (e0a) of cvo_node1.

5. Create an iSCSI LIF on node 2.

   ```
   network interface create -vserver svm_2 -service-policy default-data-
   blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
   ip_node2_iscsi_2 -home-node cvo-node2
   ```

   - This iSCSI LIF is required to support LIF migration of the floating IPs in the storage VM. It doesn’t have to be an iSCSI LIF, but it can’t be configured to migrate between nodes.
   - `-service-policy default-data-block` indicates that an IP address does not migrate between nodes.
   - *private_ip* is an unused secondary private IP address on eth0 (e0a) of cvo_node2.

6. Assign one or more aggregates to the storage VM.

   ```
   vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
   ```

   This step is required because the new storage VM needs access to at least one aggregate before you can create volumes on the storage VM.

7. If you’re running Cloud Volumes ONTAP 9.11.1 or later, modify the network service policies for the storage VM.

   Modifying the services is required because it ensures that Cloud Volumes ONTAP can use the iSCSI LIF for outbound management connections.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

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

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

To create and manage additional data-serving storage VMs in Azure, you should use the 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

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

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

To create and manage additional data-serving storage VMs in Google Cloud, you should use the 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 9.11.1, based on your license, multiple storage VMs are supported with specific configurations. Refer to the Cloud Volumes ONTAP Release Notes to verify the supported number of storage VMs for your version of Cloud Volumes ONTAP.

All versions of Cloud Volumes ONTAP prior to 9.11.1 support one data-serving storage VM and one destination storage VM used for disaster recovery. You can activate the destination storage VM for data access if there's an outage on the source storage VM.

Create a storage VM

Based on your configuration and license type, you can create multiple storage VMs on a single node system or in a high-availability (HA) configuration by using the 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 HA pairs. The required permissions are included in the policies provided by NetApp.

Single node system

Use the following API call to create a storage VM on a single node system.

`POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm`

Include the following parameters in the request body:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

HA pair

Use the following API call to create a storage VM on an HA pair:

`POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/`

Include the following parameters in the request body:

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

Manage storage VMs

Using the 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 HA pairs. The required permissions are included in the policies provided by NetApp.

Rename a storage VM

To rename a storage VM, you should provide the names of the existing storage VM and new storage VM as parameters.

Steps

- Use the following API call to rename a storage VM on a single node system:

  ```
  PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm
  ```

  Include the following parameters in the request body:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- Use the following API call to rename a storage VM on an HA pair:

  ```
  PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm
  ```

  Include the following parameters in the request body:

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

Delete a storage VM

In a single node or HA configuration, you can remove a storage VM if it doesn’t have any active volumes.

Steps

- Use the following API call to delete a storage VM on a single node system:

  ```
  DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

- Use the following API call to delete a storage VM on an HA pair:

  ```
  DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

Related information

- Prepare to use the API
- Cloud Volumes ONTAP workflows
- Get required identifiers
- Use the 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:

- AWS Key Management Service (beginning in 9.12.0)
- Azure Key Vault (AKV)
- Google Cloud Key Management Service

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

Cloud Volumes ONTAP doesn’t support onboard key management.

Before you begin

Your Cloud Volumes ONTAP system should be registered with NetApp Support. A NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support.

- Adding NetApp Support Site accounts to 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.
   - AWS: AWS Key Management Service
   - Azure: Azure Key Vault (AKV)
   - Google Cloud: Google Cloud Key Management Service

Manage Cloud Volumes ONTAP encryption keys with AWS Key Management Service

You can use AWS's Key Management Service (KMS) to protect your ONTAP encryption keys in an AWS-deployed application.

Key management with the AWS KMS can be enabled with the CLI or the ONTAP REST API.

When using the KMS, be aware that by default a data SVM's LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with AWS's authentication services. If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

Before you begin

- Cloud Volumes ONTAP must be running version 9.12.0 or later
- You must have installed the Volume Encryption (VE) license and
- You must have installed the Multi-tenant Encryption Key Management (MTEKM) license installed.
- You must be a cluster or SVM administrator
- You must have an active AWS subscription

You can only configure keys for a data SVM.

Configuration

AWS

1. You must create a grant for the AWS KMS key that will be used by the IAM role managing encryption. The IAM role must include a policy that allows the following operations:
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`
   To create a grant, refer to AWS documentation.
2. Add a policy to the appropriate IAM role. The policy should support the `DescribeKey`, `Encrypt`, and `Decrypt` operations.

Cloud Volumes ONTAP

1. Switch to your Cloud Volumes ONTAP environment.
2. Switch to the advanced privilege level:

```
set -privilege advanced
```

3. Enable the AWS key manager:
   ```
   security key-manager external aws enable -vserver data_svm_name -region
   AWS_region -key-id key_ID -encryption-context encryption_context
   ```
4. When prompted, enter the secret key.
5. Confirm the AWS KMS was configured correctly:
   ```
   security key-manager external aws show -vserver svm_name
   ```

Manage Cloud Volumes ONTAP encryption keys with Azure Key Vault

You can use Azure Key Vault (AKV) to protect your ONTAP encryption keys in an Azure-deployed application. Refer to the Microsoft documentation.

AKV can be used to protect NetApp Volume Encryption (NVE) keys only for data SVMs. For more information, refer to the ONTAP documentation.

Key management with AKV can be enabled with the CLI or the ONTAP REST API.

When using AKV, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (login.microsoftonline.com). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

Before you begin

- Cloud Volumes ONTAP must be running version 9.10.1 or later
- Volume Encryption (VE) license installed (NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support)
- You must have a Multi-tenant Encryption Key Management (MT_EK_MGMT) license
- You must be a cluster or SVM administrator
- An Active Azure subscription

Limitations

- AKV can only be configured on a data SVM
- NAE can't be used using AKV. NAE requires an external-supported KMIP server.
- Cloud Volumes ONTAP nodes poll AKV every 15 minutes to confirm accessibility and key availability. This polling period is non-configurable, and after four consecutive failures in the polling attempt (totaling 1 hour), the volumes are placed offline.

Configuration process

The outlined steps capture how to register your Cloud Volumes ONTAP configuration with Azure and how to create an Azure Key Vault and keys. If you have already completed these steps, ensure you have the correct configuration settings, particularly in Create an Azure Key Vault, and then proceed to Cloud Volumes ONTAP configuration.

- Azure Application Registration
- Create Azure client secret
- Create an Azure Key Vault

- Create encryption key
- Create an Azure Active Directory Endpoint (HA only)
- Cloud Volumes ONTAP configuration

Azure Application Registration

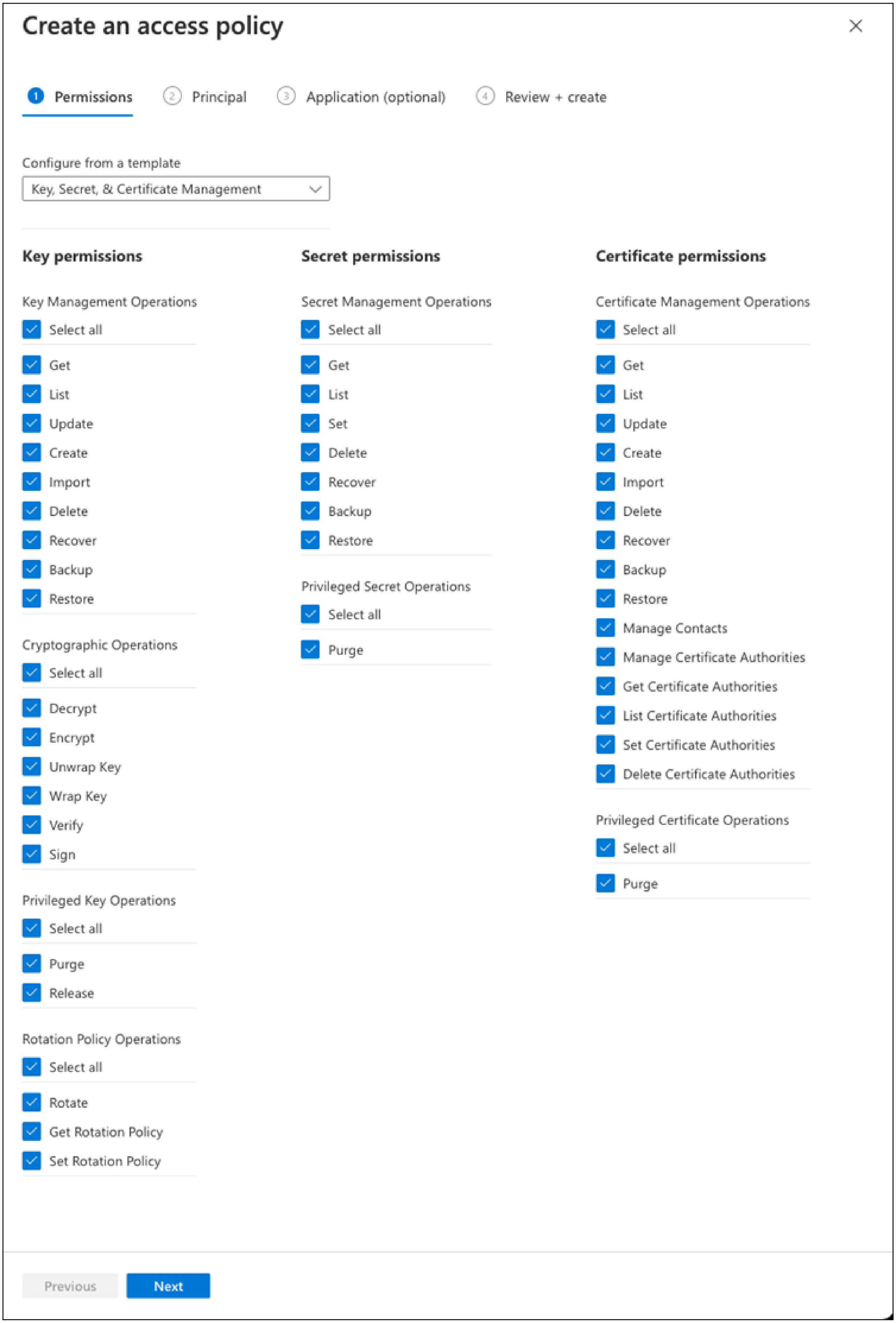
1. You must first register your application in the Azure subscription that you want the Cloud Volumes ONTAP to use for access the Azure Key Vault. Within the Azure portal, select **App registrations**.
2. Select **New registration**.
3. Provide a name for your application and select a supported application type. The default single tenant suffices for Azure Key Vault usage. Select **Register**.
4. In the Azure Overview window, select the application you have registered. Copy the **application (client) ID** and the **directory (tenant) ID** to a secure location. They will be required later in the registration process.

Create Azure client secret

1. In the Azure portal for your Azure Key Vault app registration, select the **Certificates & secrets** pane.
2. Select **New client secret**. Enter a meaningful name for your client secret. NetApp recommends a 24-month expiration period; however, your specific cloud governance policies may require a different setting.
3. Click **Add** to create the client secret. Copy the secret string listed in the **Value** column and store it in a secure location for use later in Cloud Volumes ONTAP configuration. The secret value will not be displayed again after you navigate away from the page.

Create an Azure Key Vault

1. If you have an existing Azure Key Vault, you can connect it to your Cloud Volumes ONTAP configuration; however, you must adapt the access policies to the settings in this process.
2. In the Azure portal, navigate to the **Key Vaults** section.
3. Click **+Create** and enter the required information including resource group, region, and pricing tier. In addition, enter the number of days to retain deleted vaults and select **Enable purge protection** on the key vault.
4. Select **Next** to choose an access policy.
5. Select the following options:
   a. Under **Access configuration**, select the **Vault access policy**.
   b. Under **Resource access**, select **Azure Disk Encryption for volume encryption**.
6. Select **+Create** to add an access policy.
7. Under **Configure from a template**, click the drop-down menu and then select the **Key, Secret, and Certificate Management** template.
8. Choose each of the drop-down permissions menus (key, secret, certificate) and then **Select all** at the top of the menu list to select all the permissions available. You should have:
   - **Key permissions**: 20 selected
   - **Secret permissions**: 8 selected
   - **Certificate permissions**: 16 selected



Create an access policy

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

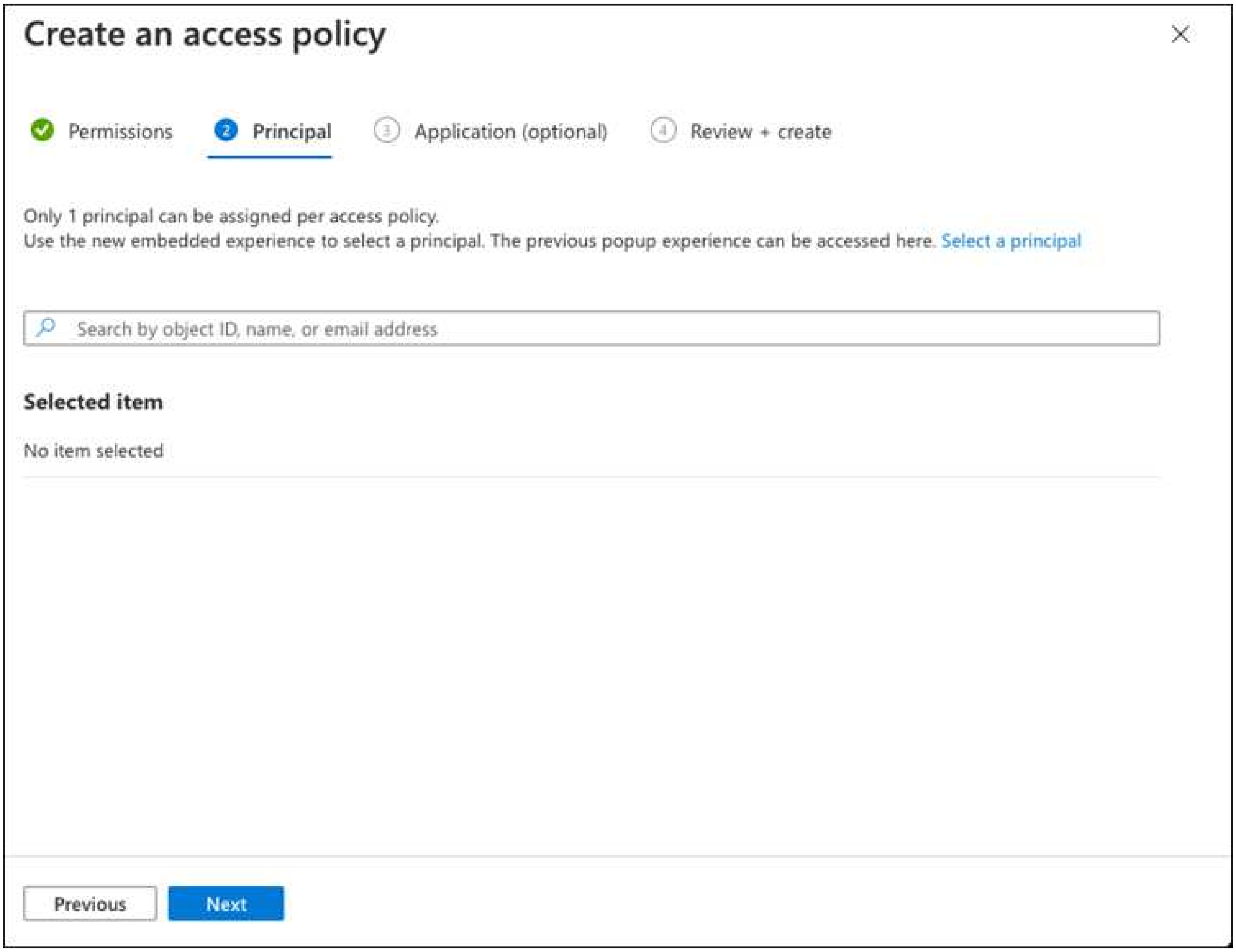
Privileged Certificate Operations

☑ Select all

☑ Purge

9. Click **Next** to select the **Principal** Azure registered application you created in Azure Application Registration. Select **Next**.

   Only one principal can be assigned per policy.



Create an access policy

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

Selected item

No item selected

10. Click **Next** two times until you arrive at **Review and create**. Then, click **Create**.
11. Select **Next** to advance to **Networking** options.
12. Choose the appropriate network access method or select **All networks** and **Review + Create** to create the key vault. (Network access method may be prescribed by a governance policy or your corporate cloud security team.)
13. Record the Key Vault URI: In the key vault you created, navigate to the Overview menu and copy the **Vault URI** from the right-hand column. You need this for a later step.

Create encryption key

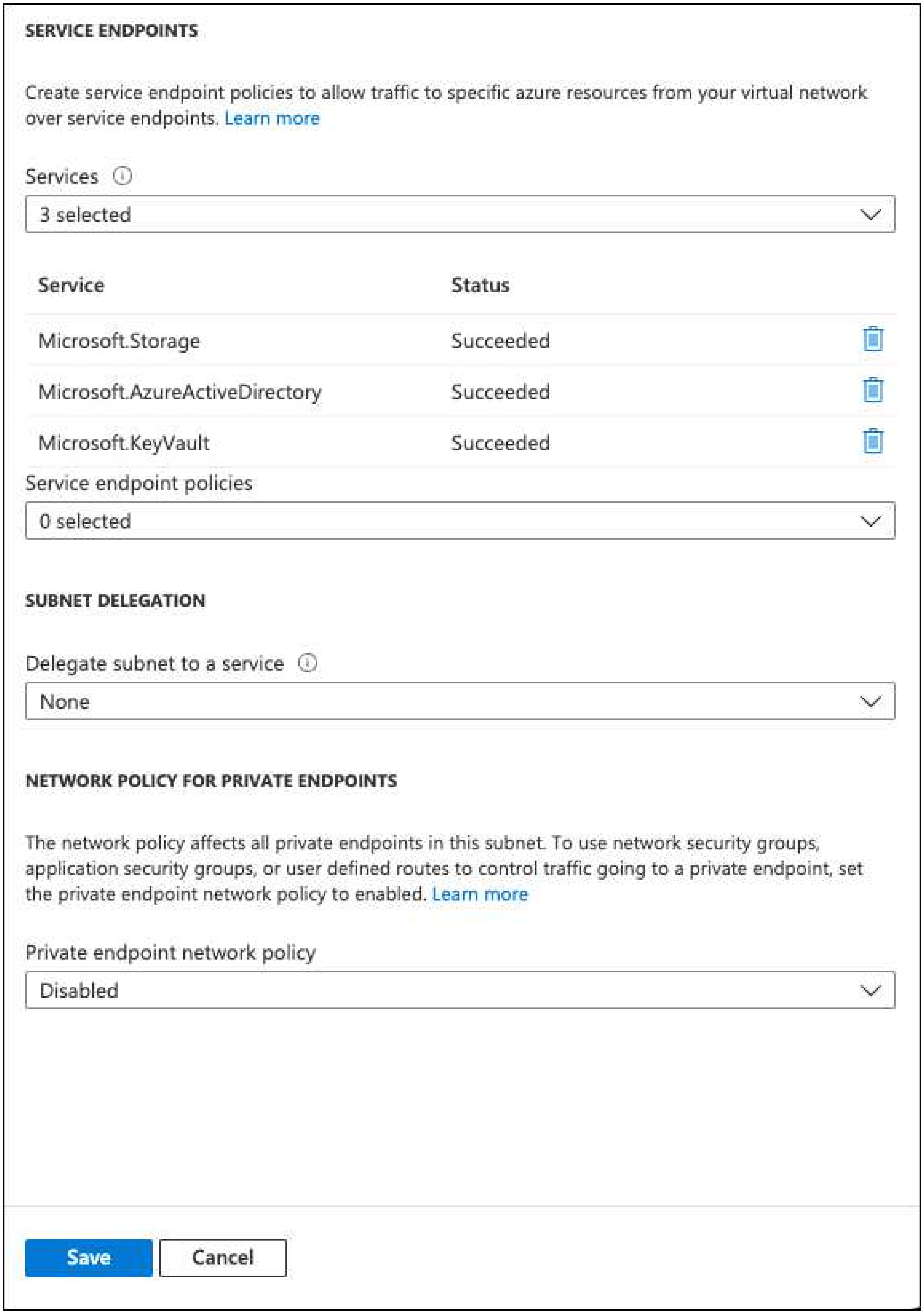
1. In the menu for the Key Vault you have created for Cloud Volumes ONTAP, navigate to the **Keys** option.
2. Select **Generate/import** to create a new key.
3. Leave the default option set to **Generate**.
4. Provide the following information:
   - Encryption key name

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

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

Create an Azure Active Directory Endpoint (HA only)

1. This process is only required if you are configuring Azure Key Vault for an HA Cloud Volumes ONTAP 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

6. Select **Save** to capture your settings.

Cloud Volumes ONTAP configuration

1. Connect to the cluster management LIF with your preferred SSH client.
2. Enter the advanced privilege mode in ONTAP:

```
set advanced -con off
```

3. Identify the desired data SVM and verify its DNS configuration:

   ```
   vserver services name-service dns show
   ```

   a. If a DNS entry for the desired data SVM exists and it contains an entry for the Azure DNS, then no action is required. If it does not, add a DNS server entry for the data SVM that points to the Azure DNS, private DNS, or on-premise server. This should match the entry for the cluster admin SVM:

      ```
      vserver services name-service dns create -vserver SVM_name -domains domain
      -name-servers IP_address
      ```

   b. Verify the DNS service has been created for the data SVM:

      ```
      vserver services name-service dns show
      ```

4. Enable Azure Key Vault using the client ID and tenant ID saved after the application registration:

   ```
   security key-manager external azure enable -vserver SVM_name -client-id
   Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id
   full_key_URI
   ```

   > The `_full_key_URI` value must utilize the `<https:// <key vault host name>/keys/<key label>` format.

5. Upon successful enablement of the Azure Key Vault, enter the `client secret value` when prompted.

6. Check the status of the key manager:

   ```
   security key-manager external azure check
   ```

   The output will look like:

   ```
   ::*> security key-manager external azure check

   Vserver: data_svm_name
   Node: akvlab01-01

   Category: service_reachability
       Status: OK

   Category: ekmip_server
       Status: OK

   Category: kms_wrapped_key_status
       Status: UNKNOWN
       Details: No volumes created yet for the vserver. Wrapped KEK status
   will be available after creating encrypted volumes.

   3 entries were displayed.
   ```

   If the `service_reachability` status is not `OK`, the SVM cannot reach the Azure Key Vault service with all the required connectivity and permissions. Ensure that your Azure network policies and routing don’t block your private vNet from reaching the Azure Key Vault Public endpoint. If they do, consider using an Azure Private endpoint to access the Key vault from within the vNet. You may also need to add a static hosts entry on your SVM to resolve the private IP address for your endpoint.

The `kms_wrapped_key_status` will report `UNKNOWN` at initial configuration. Its status will change to `OK` after the first volume is encrypted.

7. OPTIONAL: Create a test volume to verify the functionality of NVE.

   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```

   If configured correctly, Cloud Volumes ONTAP will automatically create the volume and enable volume encryption.

8. Confirm the volume was created and encrypted correctly. If it is, the `-is-encrypted` parameter will display as `true`.

   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```

9. Optional: If you want to update the credentials on the Azure Key Vault authentication certificate, use the following command:

   ```
   security key-manager external azure update-credentials -vserver v1
   -authentication-method certificate
   ```

Related links

- Set up Cloud Volumes ONTAP to use a customer-managed key in Azure
- Microsoft Azure docmentation: About Azure Key Vault
- ONTAP command reference guide

Manage Cloud Volumes ONTAP encryption keys with Google Cloud KMS

You can use Google Cloud Platform's Key Management Service (Cloud KMS) to protect your Cloud Volumes ONTAP encryption keys in a Google Cloud Platform-deployed application.

Key management with Cloud KMS can be enabled with the ONTAP CLI or the ONTAP REST API.

When using Cloud KMS, be aware that by default a data SVM's LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (oauth2.googleapis.com). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

Before you begin

- Your system should be running Cloud Volumes ONTAP 9.10.1 or later
- You must use a data SVM. Cloud KMS can be configured only on a data SVM.
- You must be a cluster or SVM administrator
- Volume Encryption (VE) license should be installed on the SVM
- Beginning with Cloud Volumes ONTAP 9.12.1 GA, the multi-tenant Encryption Key Management (MTEKM) license should also be installed
- An active Google Cloud Platform subscription is required

Configuration

Google Cloud

1. In your Google Cloud environment, create a symmetric GCP key ring and key.
2. Assign a custom role to the Cloud KMS key and Cloud Volumes ONTAP service account.
   a. Create the custom role:

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

   b. Assign the custom role you created:
   `gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name --location key_location --member serviceAccount:_service_account_Name_ --role projects/customer_project_id/roles/kmsCustomRole`

   If you are on Cloud Volumes ONTAP 9.13.0 or later, you don't need to create a custom role. You can assign the predefined `cloudkms.cryptoKeyEncrypterDecrypter` role.

3. Download service account JSON key:
   `gcloud iam service-accounts keys create key-file --iam-account=sa-name @project-id.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. Connect to the cluster management LIF with your preferred SSH client.
2. Switch to the advanced privilege level:
   `set -privilege advanced`
3. Create a DNS for the data SVM.
   `dns create -domains c.<project>.internal -name-servers server_address -vserver SVM_name`
4. Create CMEK entry:
   `security key-manager external gcp enable -vserver SVM_name -project-id project -key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
5. When prompted, enter the service account JSON key from your GCP account.
6. Confirm the enabled process succeeded:
   `security key-manager external gcp check -vserver svm_name`
7. OPTIONAL: Create a volume to test encryption `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

Troubleshoot

If you need to troubleshoot, you can tail the raw REST API logs in the final two steps above:

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Enable NetApp ransomware protection solutions for Cloud Volumes ONTAP

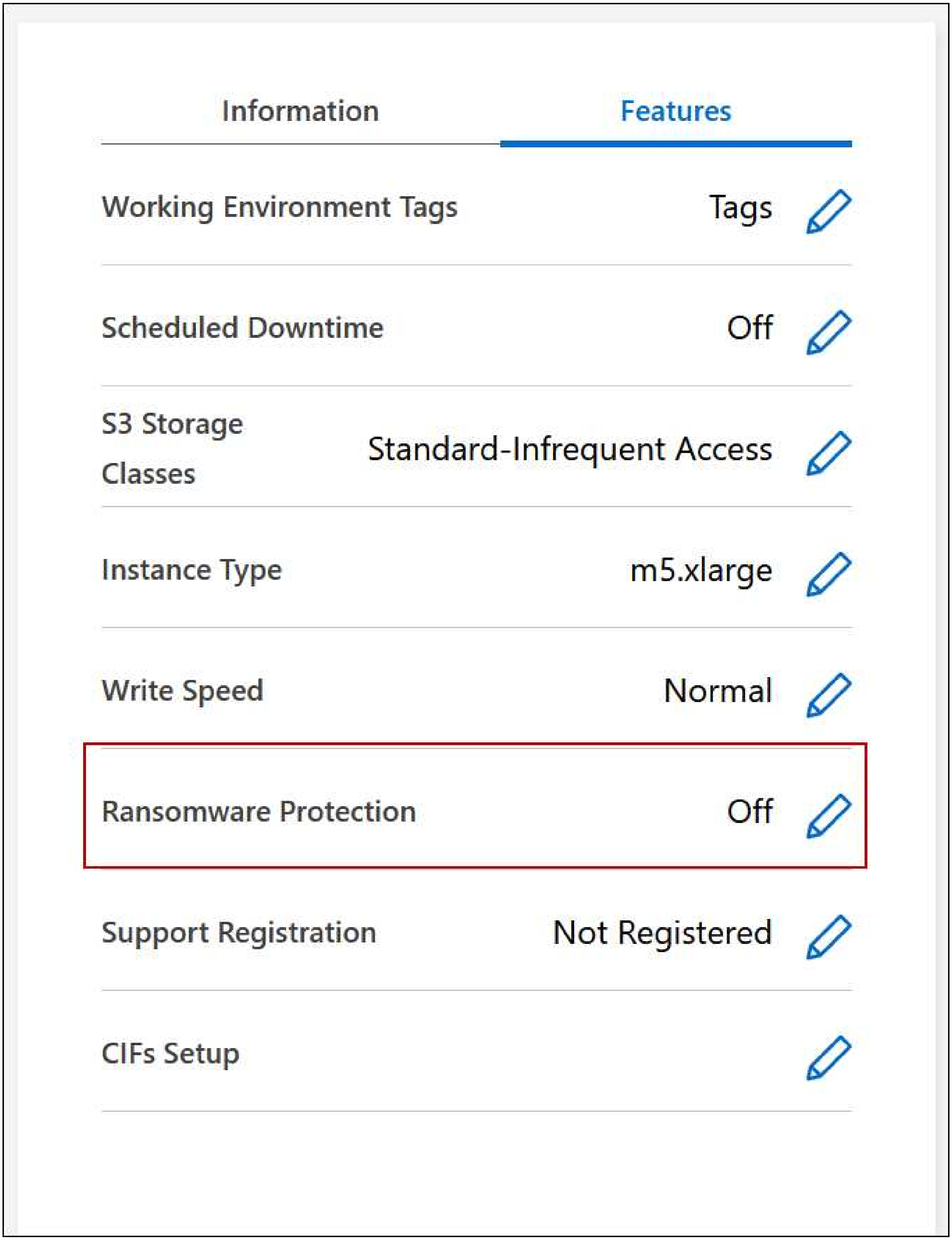
Ransomware attacks can cost a business time, resources, and reputation. BlueXP enables you to implement two NetApp solutions for ransomware: Protection from common ransomware file extensions and Autonomous Ransomware Protection (ARP). These solutions provide effective tools for visibility, detection, 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**.



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:
   a. Click **Activate Snapshot Policy**, if you have volumes that do not have a Snapshot policy enabled.

NetApp Snapshot technology provides the industry’s best solution for ransomware remediation. The key to a successful recovery is restoring from uninfected backups. Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

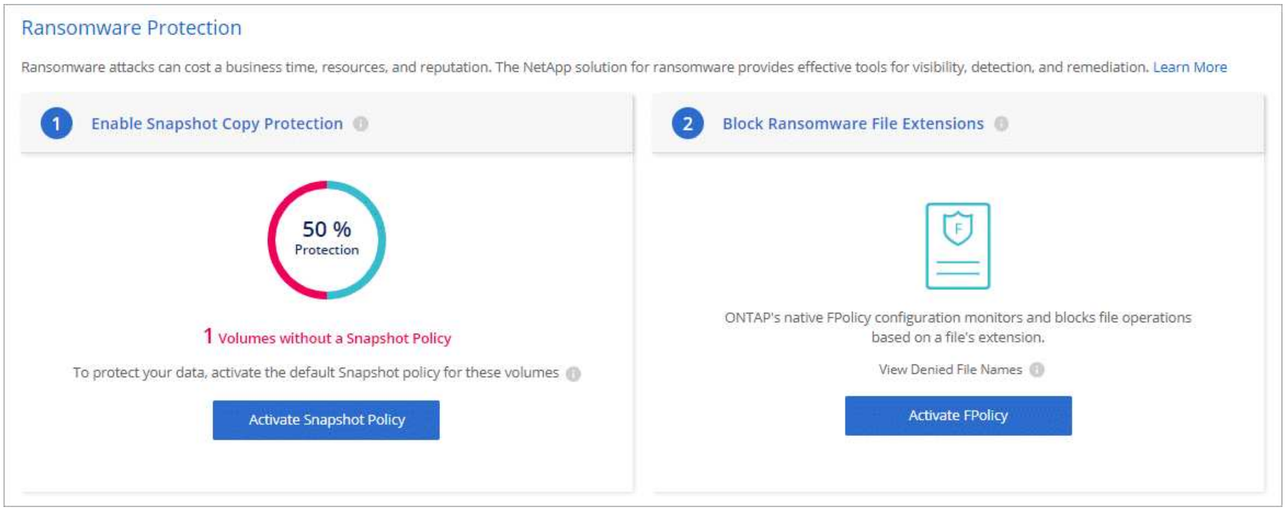
b. Click **Activate FPolicy** to enable ONTAP’s FPolicy solution, which can block file operations based on a file’s extension.

   This preventative solution improves protection from ransomware attacks by blocking common ransomware file types.

   The default FPolicy scope blocks files that have the following extensions:

   micro, encrypted, locked, crypto, crypt, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, good, LOL!, OMG!, RDM, RRK, encryptedRS, crjoker, EnCiPhErEd, LeChiffre

   > 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

1 Volumes without a Snapshot Policy

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

2 Block Ransomware File Extensions

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

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.

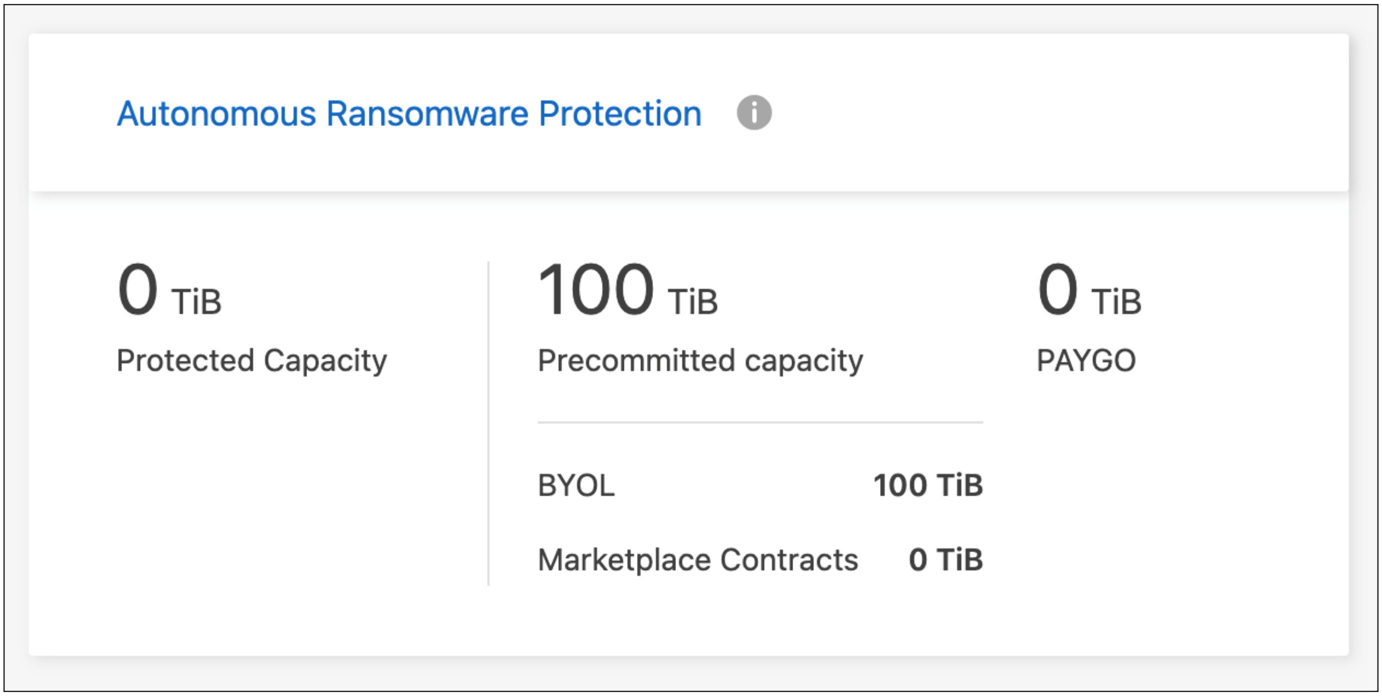
Separate from the file extension protections provided through the ransomware protection setting, the ARP feature uses workload analysis to alert the user on potential attacks based on detected “abnormal activity”. Both the ransomware protection setting and the ARP feature can be used in conjunction for 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.



Autonomous Ransomware Protection

0 TiB
Protected Capacity

100 TiB
Precommitted capacity

BYOL	100 TiB
Marketplace Contracts	0 TiB

0 TiB
PAYGO

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
9.15.1	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
9.11.1	9.12.1
	9.12.0

Current version	Versions that you can directly upgrade to
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Note the following:

- The supported upgrade paths for Cloud Volumes ONTAP are different than they are for an on-premises ONTAP cluster.
- If you upgrade by following the upgrade notifications that appear in a working environment, 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.

The computer from which you are accessing BlueXP must have a network connection to Cloud Volumes ONTAP. For example, you might need to log in to BlueXP from a jump host that's in your cloud provider network.

2. Click **Protection > Relationships**.
3. Select the relationship and click **Operations > Quiesce**.

Verify that aggregates are online

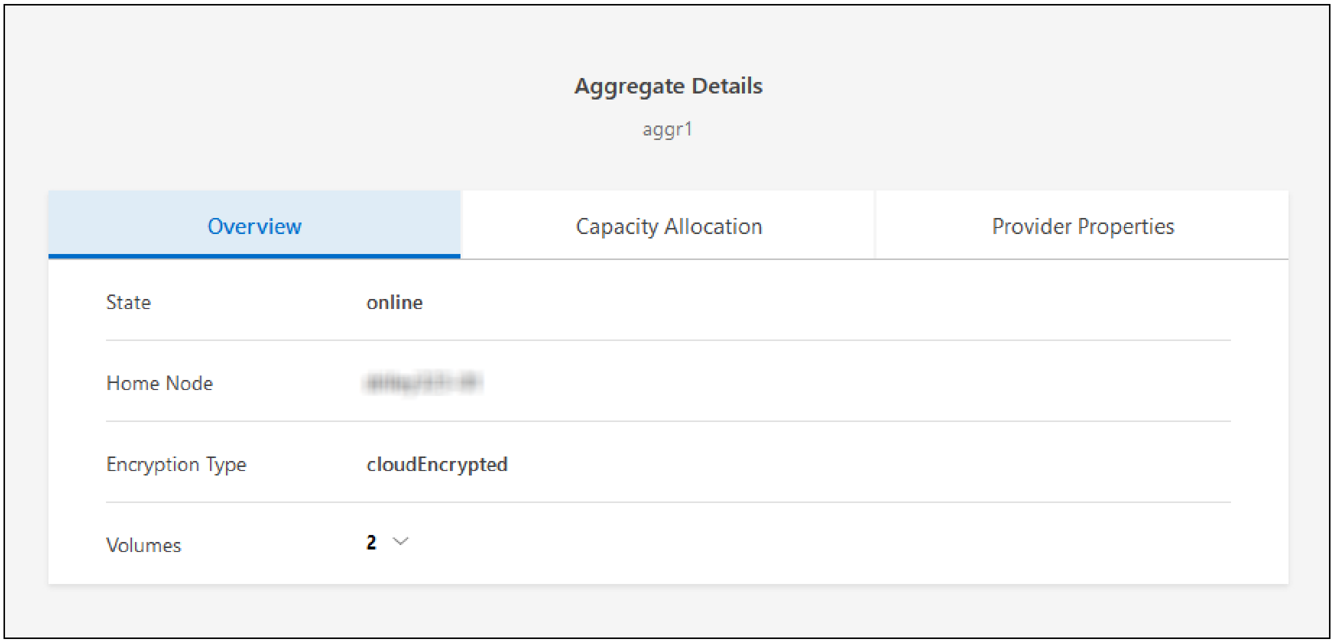
Aggregates for Cloud Volumes ONTAP must be online before you update the software. Aggregates should be online in most configurations, but if they are not, then you should bring them online.

About this task

These steps describe how to use ONTAP System Manager for version 9.3 and later.

Steps

1. In the working environment, click the **Aggregates** tab.
2. Under the aggregate title, click the ellipses button, and then select **View Aggregate details**.



Aggregate Details

aggr1

State	online
Home Node	[redacted]
Encryption Type	cloudEncrypted
Volumes	2

3. If the aggregate is offline, use System Manager to bring the aggregate online:
   a. Click **Storage > Aggregates & Disks > Aggregates**.
   b. Select the aggregate, and then click **More Actions > Status > Online**.

Verify that all LIFs are on home ports

Before you upgrade, all LIFs must be on home ports. Refer to the ONTAP documentation to verify that all LIFs are on home ports.

If an upgrade failure error occurs, consult the Knowledge Base (KB) article Cloud Volumes ONTAP upgrade fails.

Upgrade Cloud Volumes ONTAP

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.

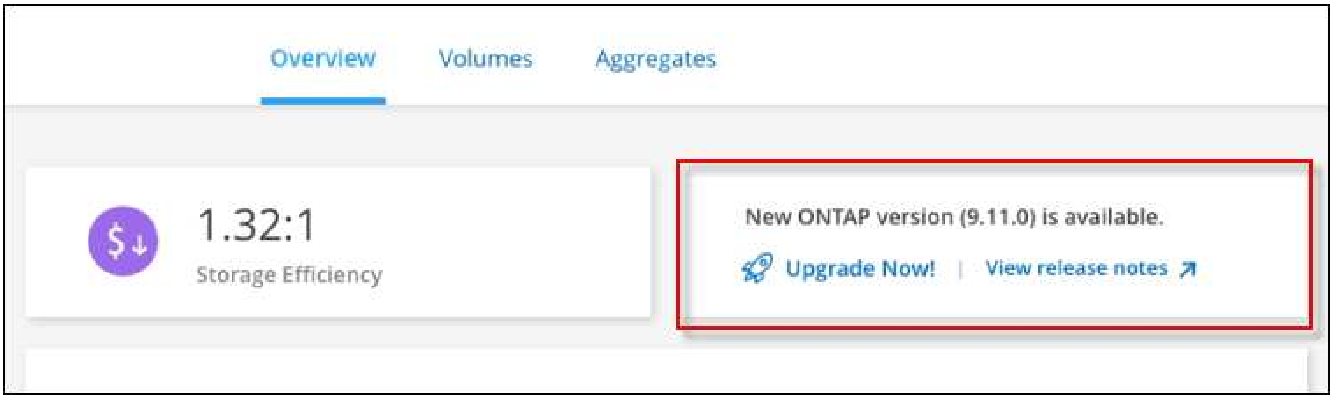
Before you begin

BlueXP operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.

Steps

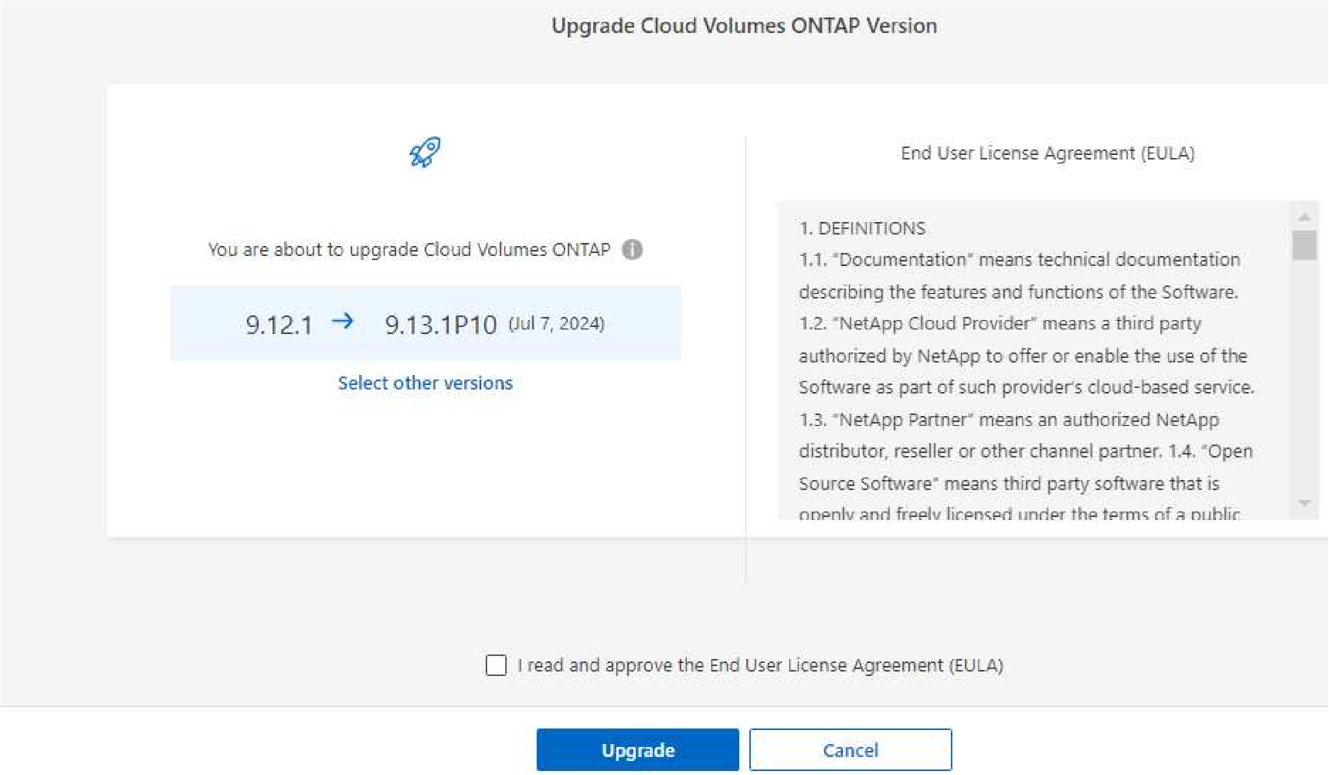
1. From the left navigation menu, select **Storage > Canvas**.
2. Select a working environment.

   A notification appears in the Overview tab if a new version is available:



New ONTAP version (9.11.0) 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)

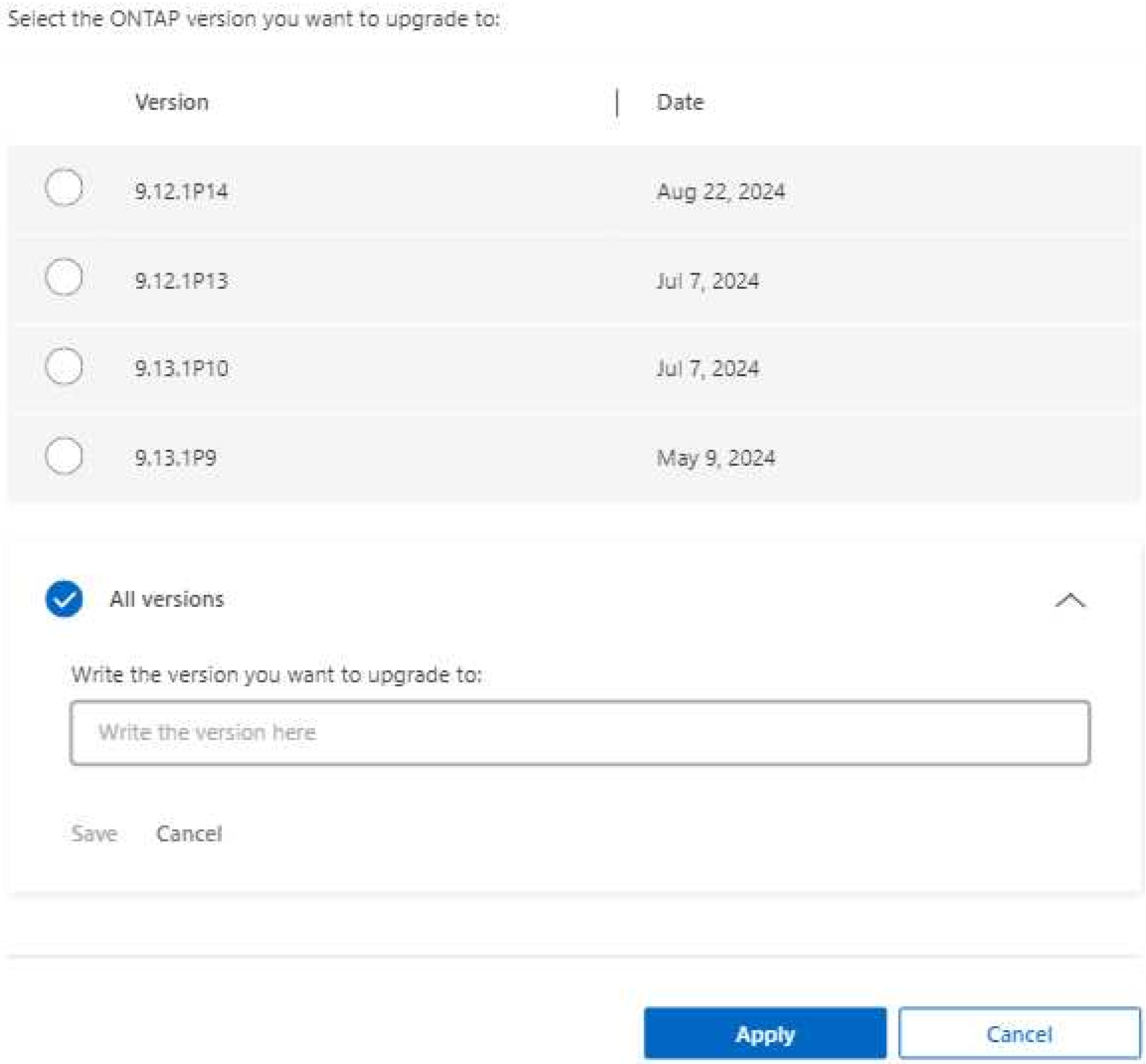
1. DEFINITIONS
1.1. "Documentation" means technical documentation describing the features and functions of the Software.
1.2. "NetApp Cloud Provider" means a third party authorized by NetApp to offer or enable the use of the Software as part of such provider's cloud-based service.
1.3. "NetApp Partner" 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)

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
○	9.12.1P14	Aug 22, 2024
○	9.12.1P13	Jul 7, 2024
○	9.13.1P10	Jul 7, 2024
○	9.13.1P9	May 9, 2024

☑ All versions

Write the version you want to upgrade to:

Write the version here

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.

Fix download failures when using a Google Cloud NAT gateway

The Connector automatically downloads software updates for Cloud Volumes ONTAP. The download can fail if your configuration uses a Google Cloud NAT gateway. You can correct this issue by limiting the number of parts that the software image is divided into. This step must be completed by using the BlueXP API.

Step

1. Submit a PUT request to /occm/config with the following JSON as body:

```
{
  "maxDownloadSessions": 32
}
```

The value for *maxDownloadSessions* can be 1 or any integer greater than 1. If the value is 1, then the downloaded image will not be divided.

Note that 32 is an example value. The value that you should use depends on your NAT configuration and the number of sessions that you can have simultaneously.

Learn more about the /occm/config API call.

Register Cloud Volumes ONTAP pay-as-you-go systems

Support from NetApp is included with Cloud Volumes ONTAP pay-as-you-go (PAYGO) systems, but you must first activate support by registering the systems with NetApp.

Registering a PAYGO system with NetApp is required to upgrade ONTAP software using any of the methods described on this page.

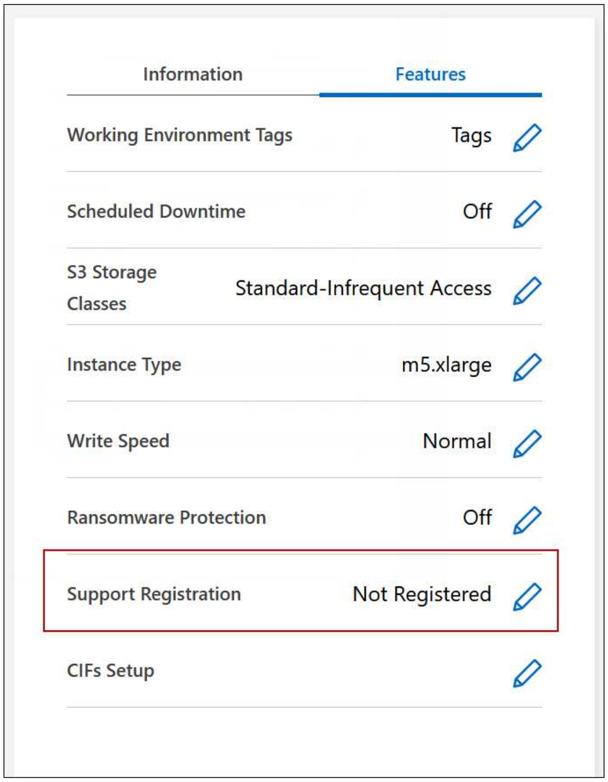
> A system that isn’t registered for support will still receive the software update notifications that appear in BlueXP when a new version is available. But you will need to register the system before you can upgrade the software.

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**.



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	

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 - awspo@netapp.com
- Azure - azurepo@netapp.com
- Google Cloud - gcppo@netapp.com

Start and stop a Cloud Volumes ONTAP system

You can stop and start Cloud Volumes ONTAP from 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.

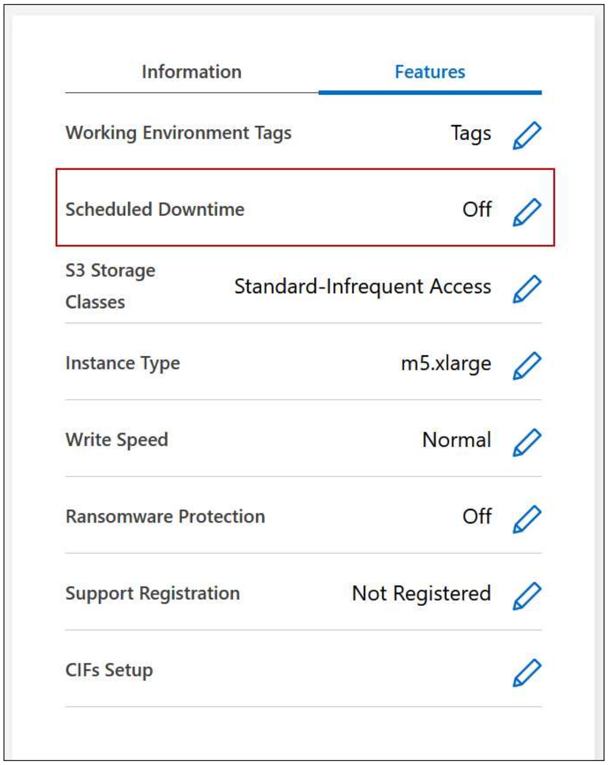
  BlueXP shuts down the system after the transfer is complete.

- 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**.

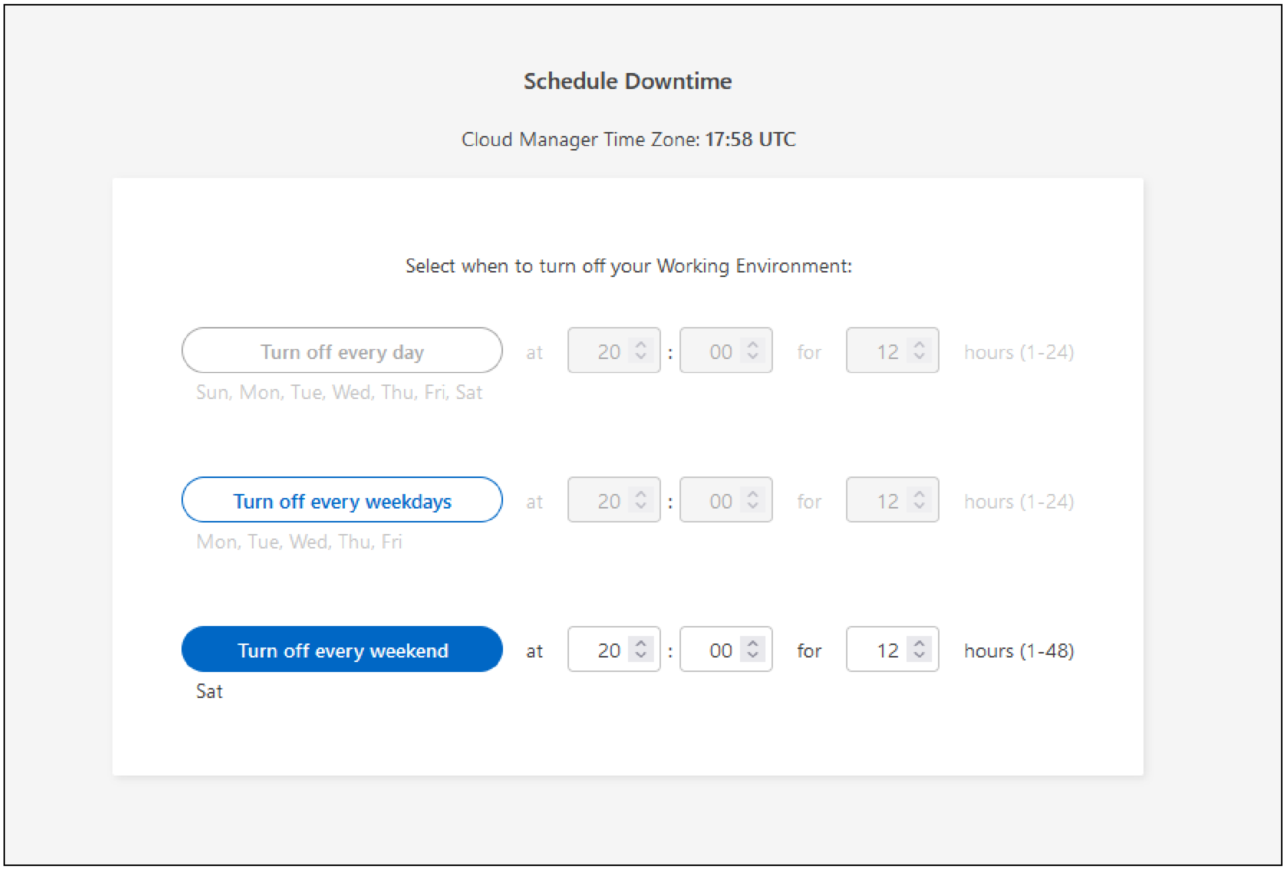
   

Working Environment Tags	Tags
Scheduled Downtime	Off
S3 Storage Classes	Standard-Infrequent Access
Instance Type	m5.xlarge
Write Speed	Normal
Ransomware Protection	Off
Support Registration	Not Registered
CIFs Setup	

3. Specify the shutdown schedule:
   a. Choose whether you want to shut down the system every day, every weekday, every weekend, or any combination of the three options.
   b. Specify when you want to turn off the system and for how long you want it turned off.

      Example

      The following image shows a schedule that instructs 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 at 20 : 00 for 12 hours (1-24)
Sun, Mon, Tue, Wed, Thu, Fri, Sat

Turn off every weekdays at 20 : 00 for 12 hours (1-24)
Mon, Tue, Wed, Thu, Fri

Turn off every weekend at 20 : 00 for 12 hours (1-48)
Sat

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.

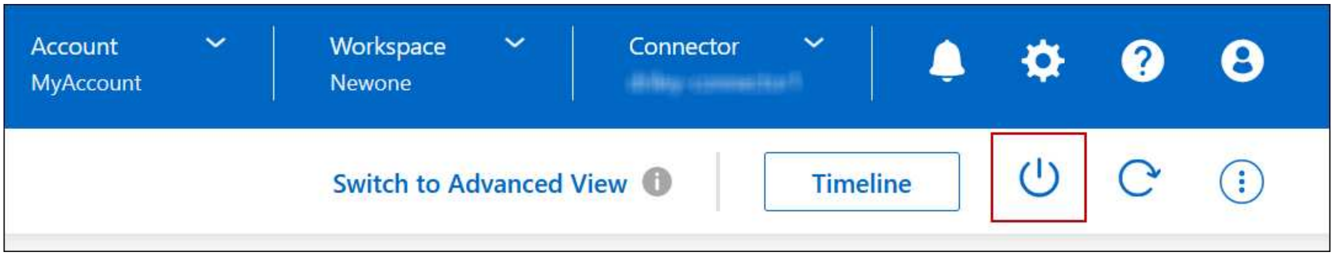
> ⓘ To reduce costs, BlueXP periodically deletes older snapshots of root and boot disks. Only the two most recent snapshots are retained for both the root and boot disks.

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

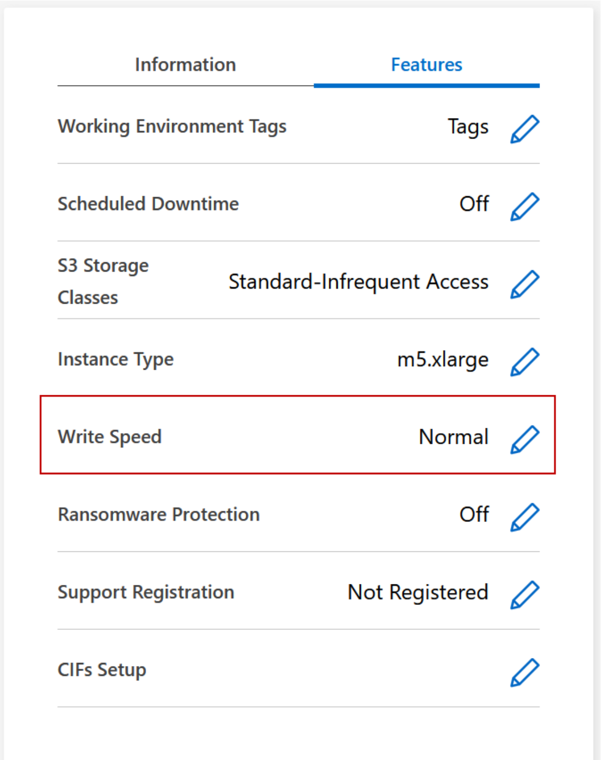
Before you change the write speed, you should understand the differences between the normal and high settings.

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**.



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.

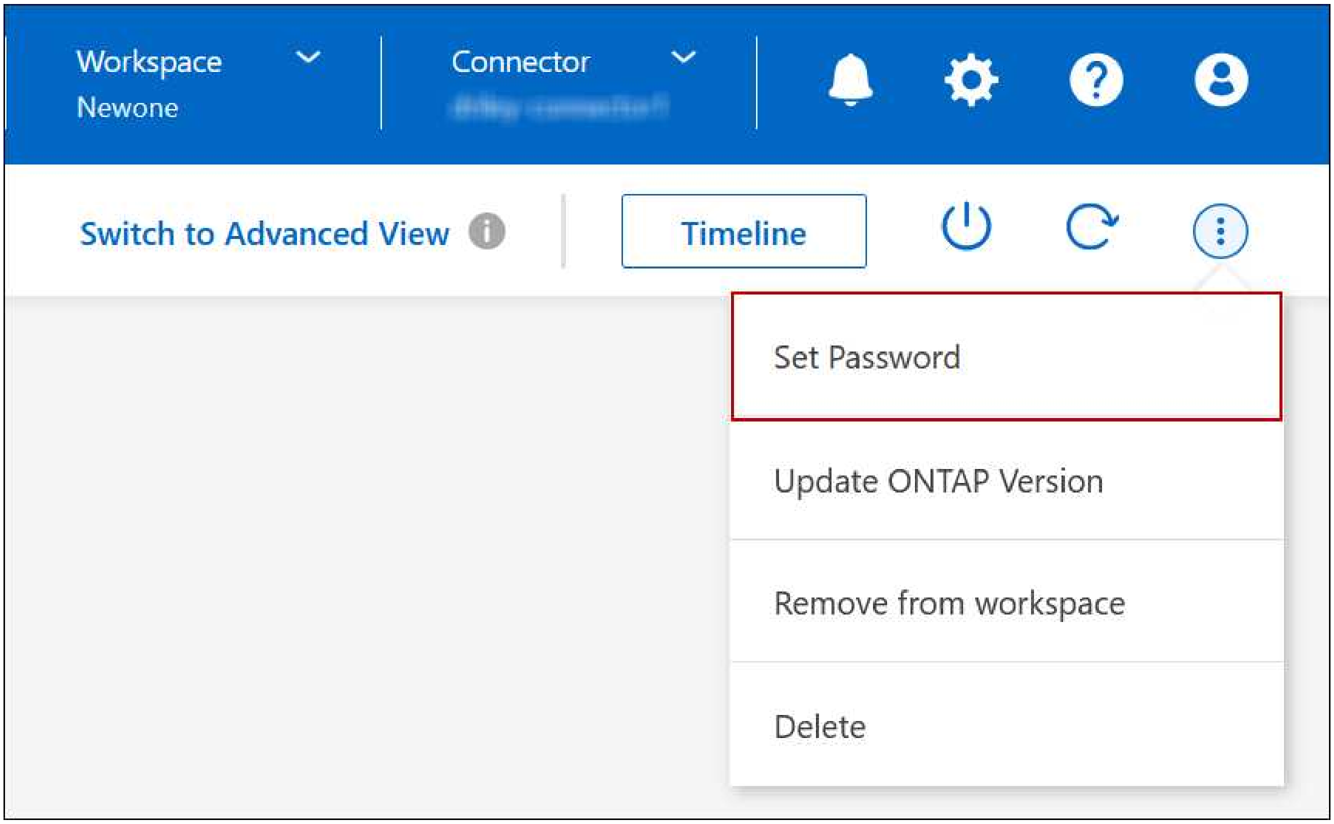
About this task

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

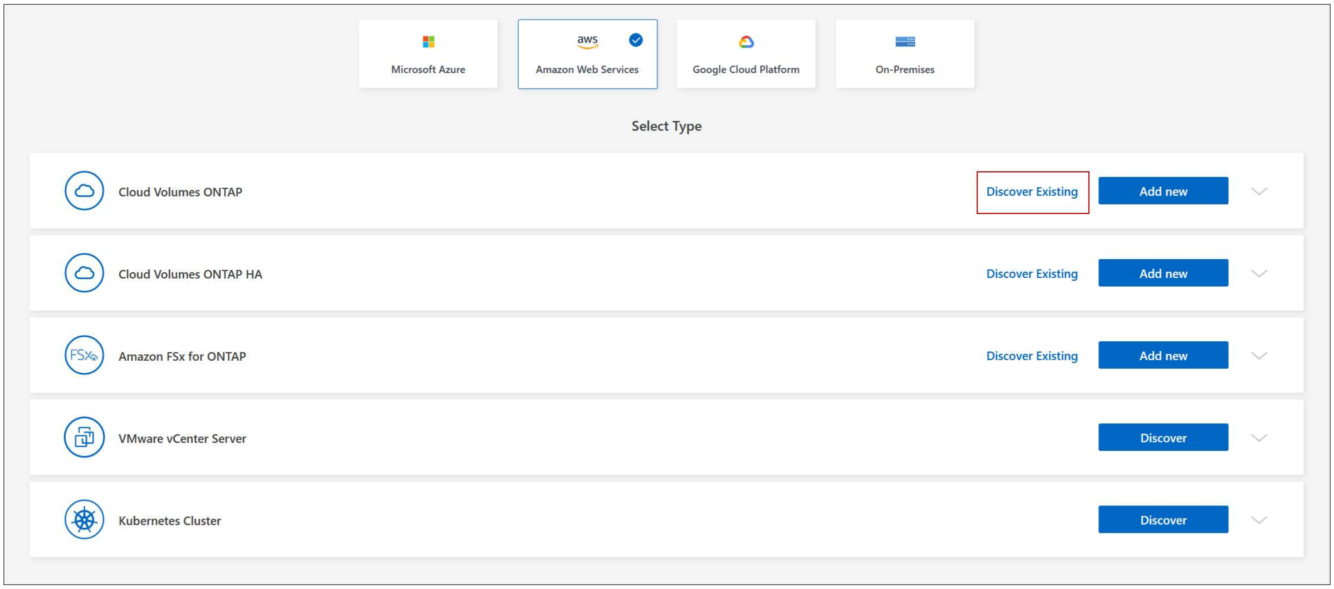
You can discover and add existing Cloud Volumes ONTAP systems to BlueXP. You might do this if you deployed a new BlueXP system.

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

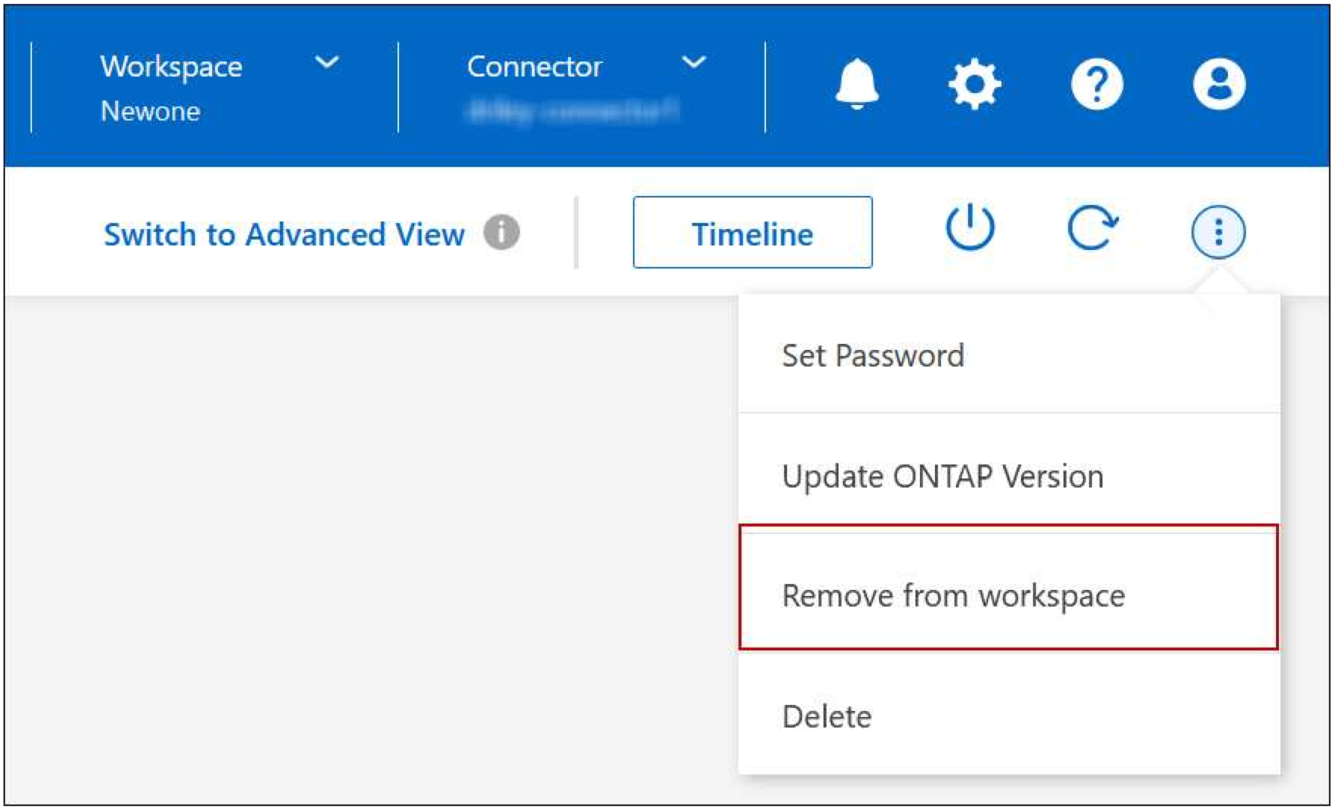
You can remove a Cloud Volumes ONTAP working environment to move it to another system or to troubleshoot discovery issues.

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.

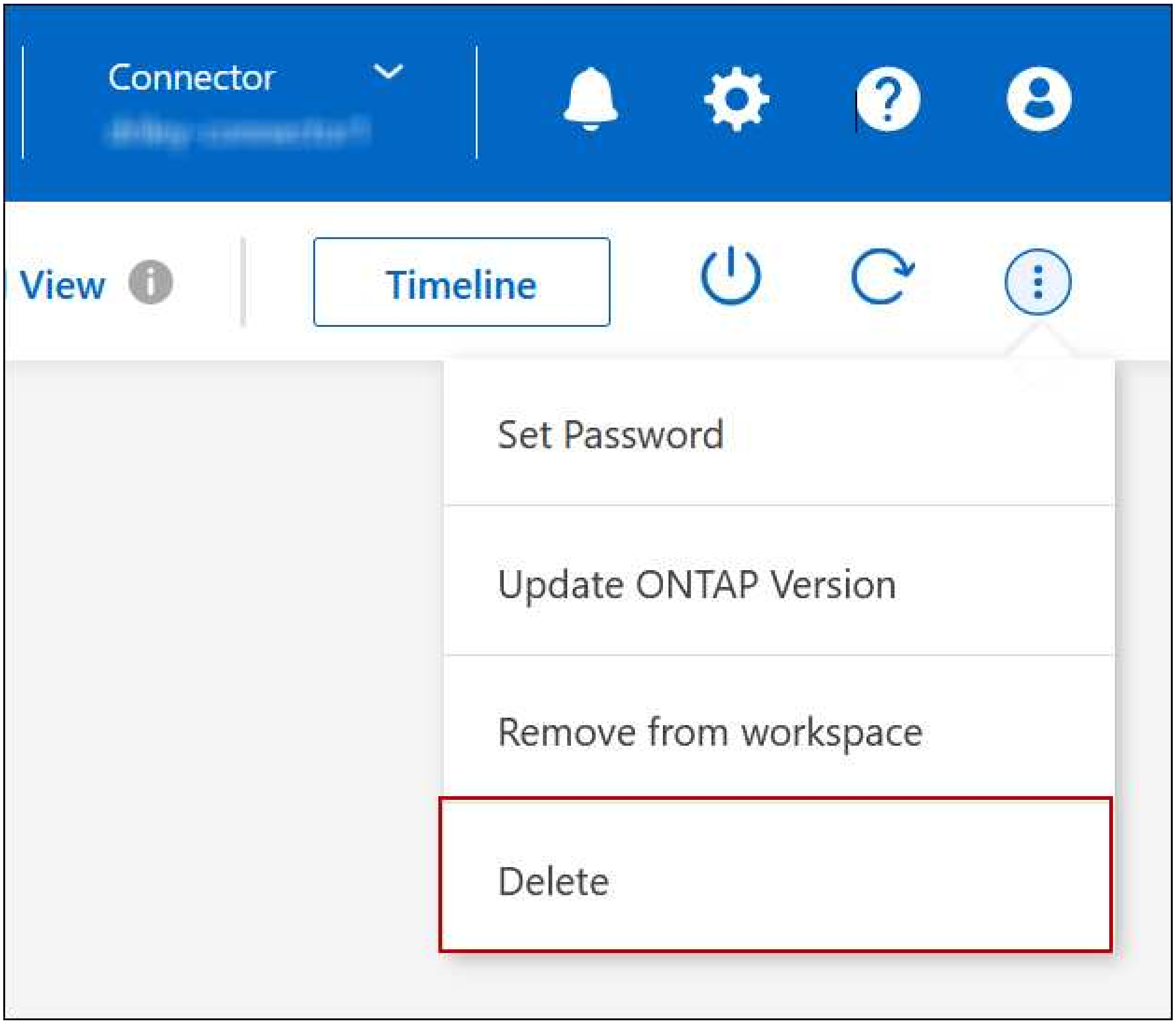
2. If you enabled BlueXP classification on this working environment and no other working environments use this service, then you’ll need to delete the instance for the service.

   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.

AWS administration

Modify the EC2 instance type for a Cloud Volumes ONTAP system in AWS

You can choose from several instance or types when you launch Cloud Volumes ONTAP in AWS. You can change the instance type at any time if you determine that it is undersized or oversized for your needs.

About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

  ONTAP 9 Documentation: Commands for configuring automatic giveback

- Changing the instance type can affect AWS service charges.
- The operation restarts Cloud Volumes ONTAP.

  For single node systems, I/O is interrupted.

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

  > 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.

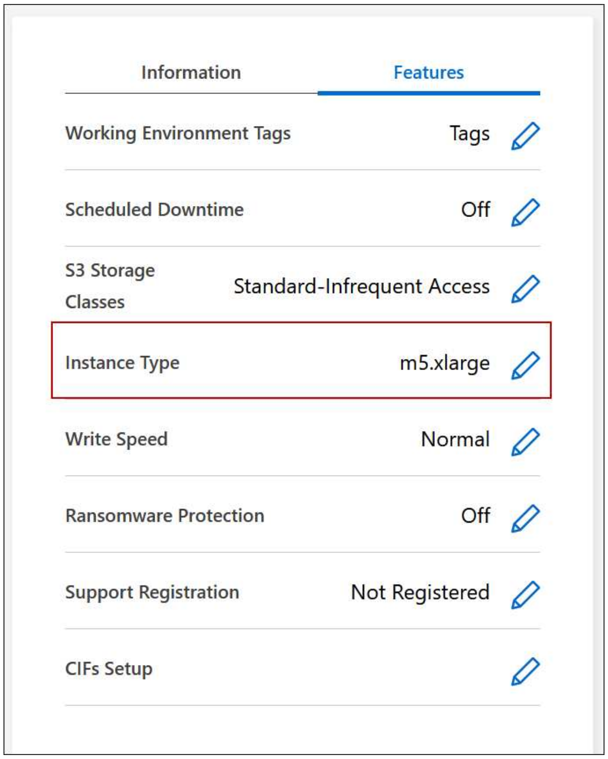
Reference

For a list of supported instance types in AWS, refer to Supported EC2 instances.

If you can't change the instance type from c4, m4, or r4 instances, refer to KB article "Converting an AWS Xen CVO instance to Nitro (KVM)".

Steps

1. On the Canvas page, select the working environment.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Instance type**.



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	

If you are using a node-based pay as you go (PAYGO) license, you can optionally choose a different license and instance type by clicking the pencil icon next to **License type**.

1. Choose an instance type, select the check box to confirm that you understand the implications of the change, and then click **Change**.

Result

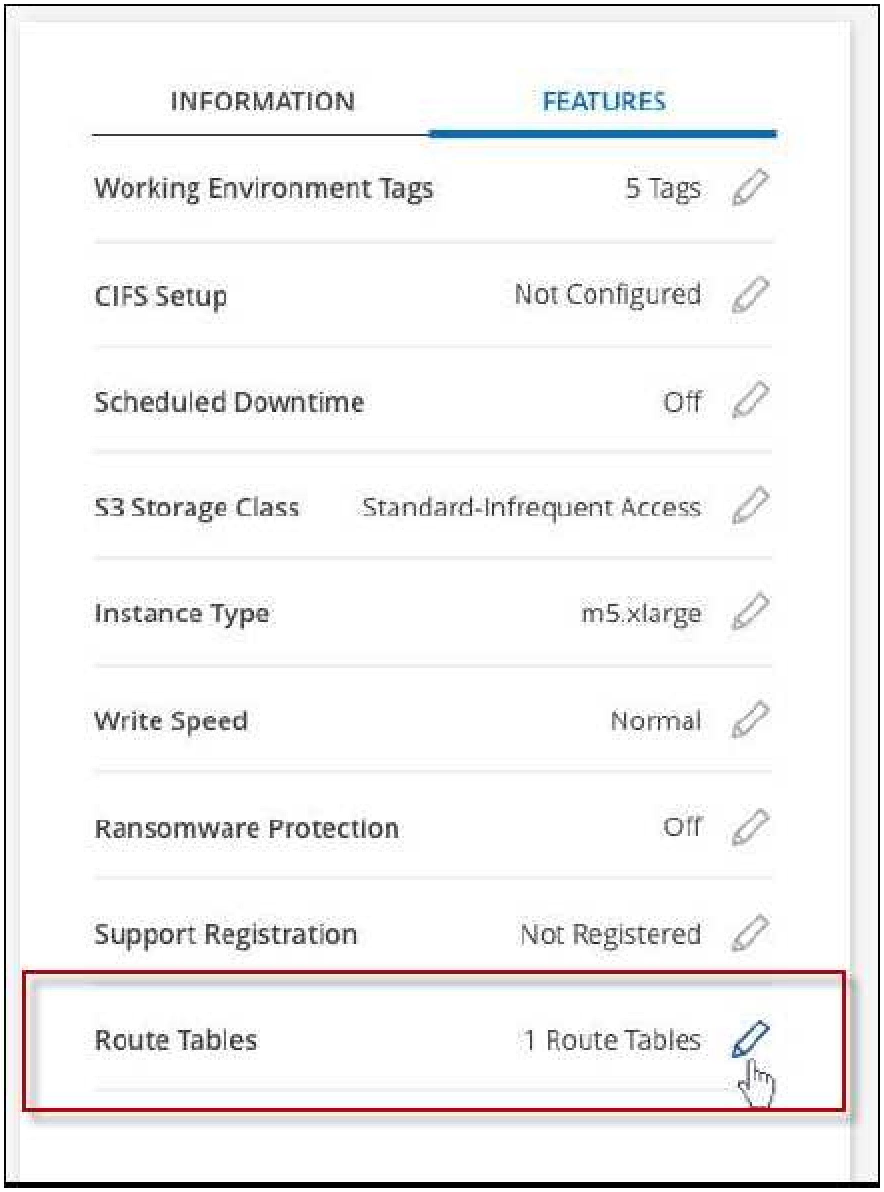
Cloud Volumes ONTAP reboots with the new configuration.

Modify route tables for Cloud Volumes ONTAP HA pairs in multiple AWS AZs

You can modify the AWS route tables that include routes to the floating IP addresses for an HA pair that's deployed in multiple AWS Availability Zones (AZs). You might do this if new NFS or CIFS clients need to access an HA pair in AWS.

Steps

1. On the Canvas page, select the working environment.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Route tables**.



Working Environment Tags	5 Tags
CIFS Setup	Not Configured
Scheduled Downtime	Off
S3 Storage Class	Standard-Infrequent Access
Instance Type	m5.xlarge
Write Speed	Normal
Ransomware Protection	Off
Support Registration	Not Registered
Route Tables	1 Route Tables

3. Modify the list of selected route tables and then click **Save**.

Result

BlueXP sends an AWS request to modify the route tables.

Azure administration

Change the Azure VM type for Cloud Volumes ONTAP

You can choose from several VM types when you launch Cloud Volumes ONTAP in Microsoft Azure. You can change the VM type at any time if you determine that it is undersized or oversized for your needs.

About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn’t, then the operation will fail.

  ONTAP 9 Documentation: Commands for configuring automatic giveback

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

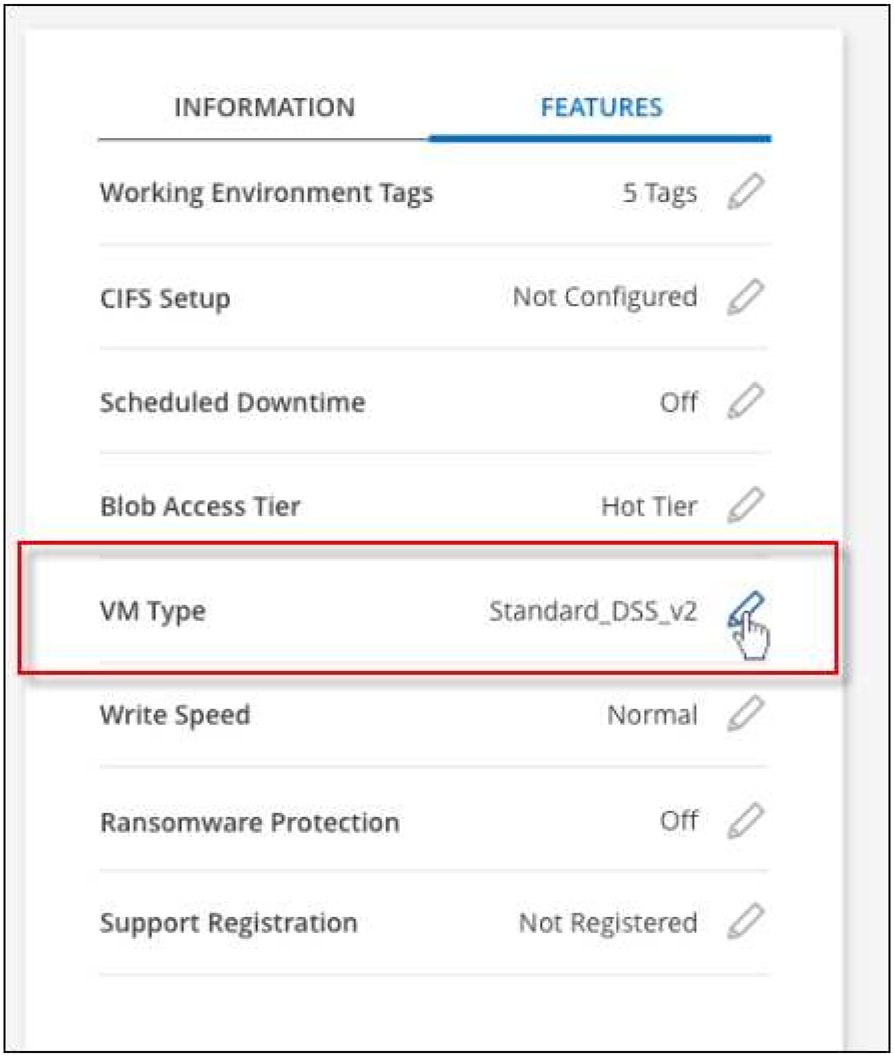
  For single node systems, I/O is interrupted.

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

  > 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**.



Working Environment Tags	5 Tags
CIFS Setup	Not Configured
Scheduled Downtime	Off
Blob Access Tier	Hot Tier
VM Type	Standard_DSS_v2
Write Speed	Normal
Ransomware Protection	Off
Support Registration	Not Registered

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.

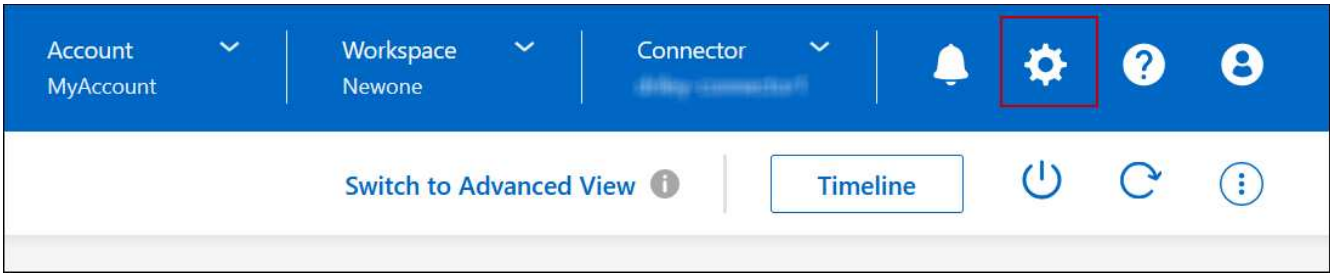
> This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

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.

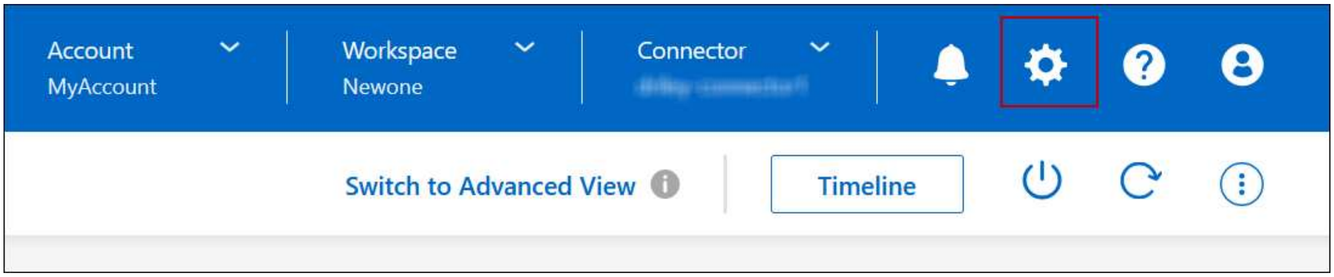
Disable Azure Private Links and use service endpoints instead

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

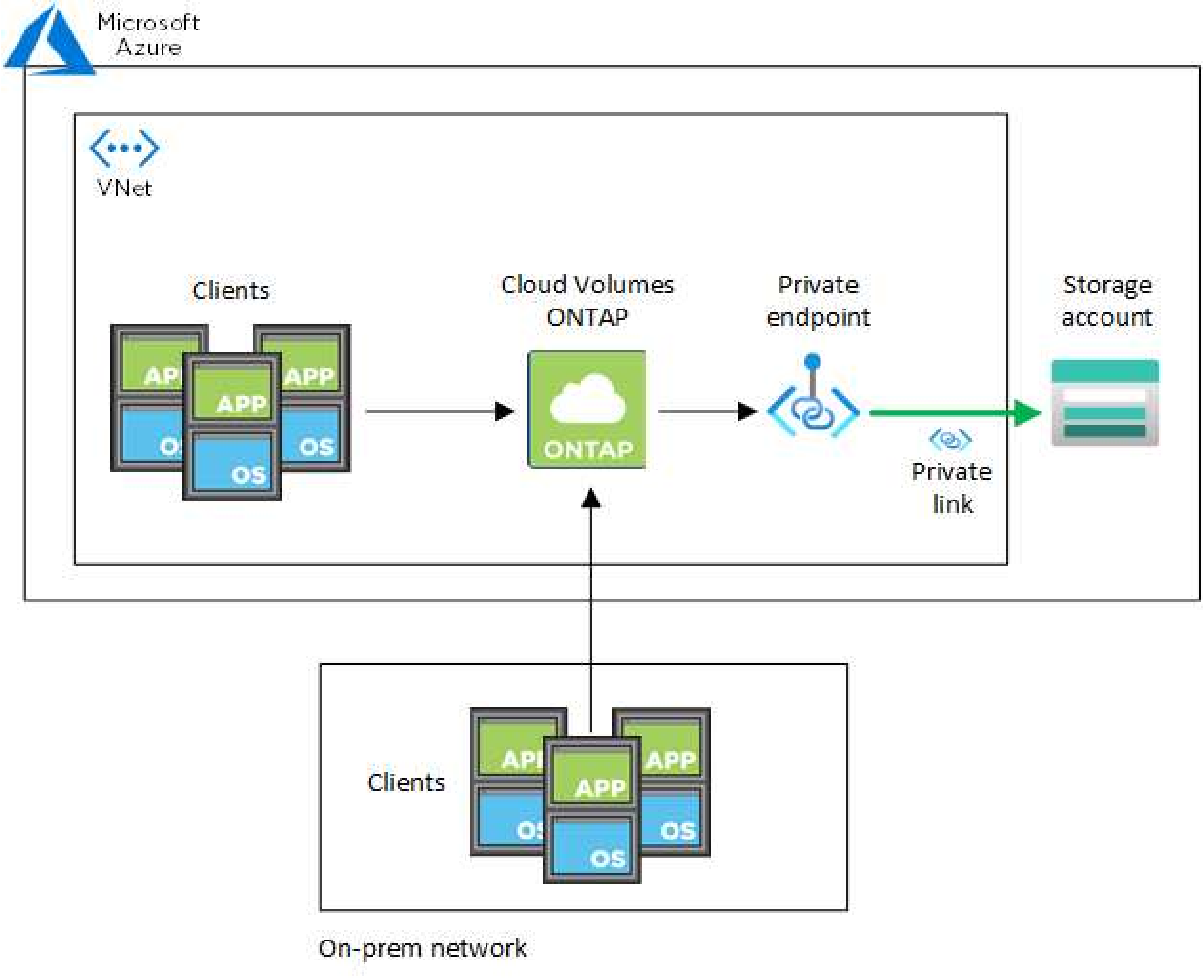
Optionally, if you work with custom DNS, you need to create a conditional forwarder to the Azure private DNS zone from your custom DNS servers. To learn more, refer to Azure’s documentation on using a DNS forwarder.

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

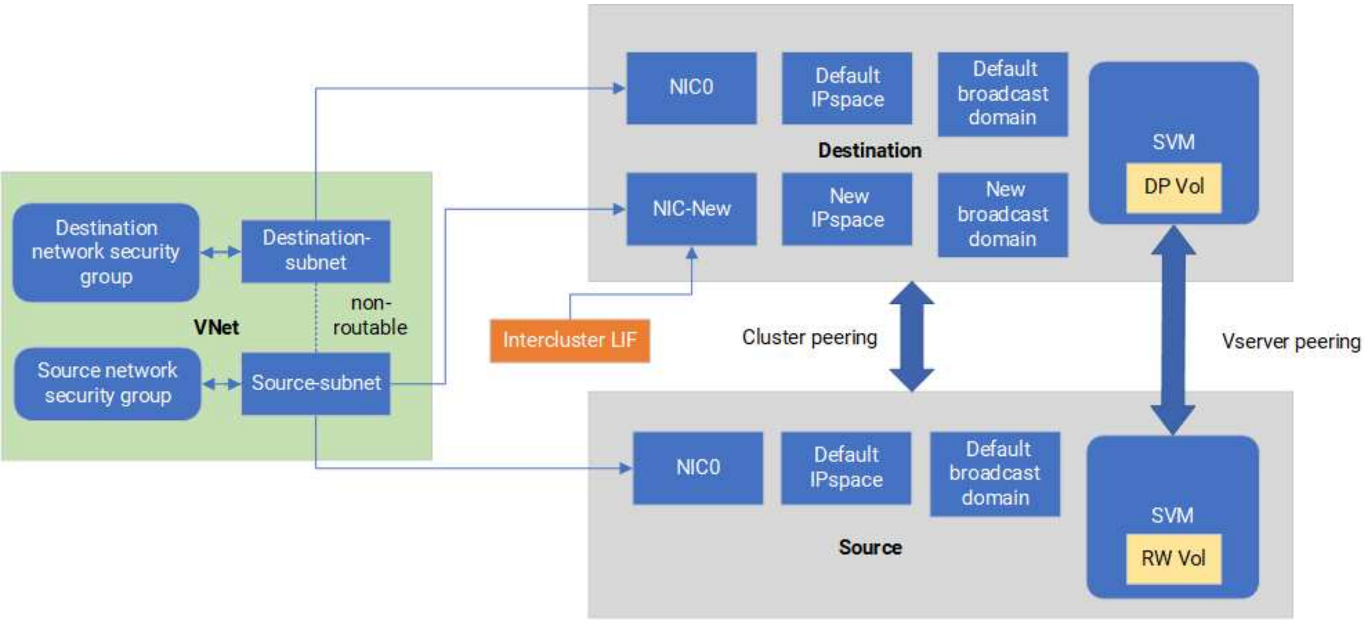
With Cloud Volumes ONTAP in Azure, you can segregate SnapMirror replication traffic from data and management traffic. To segregate SnapMirror replication traffic from your data traffic, you'll add a new network interface card (NIC), an associated intercluster LIF and a non-routable subnet.

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-addrs`. For HA pairs, list the source intercluster LIF IP address for both nodes as the `-peer-addrs`.

   ```
   dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
   <new_ipspace>
   ```

2. Enter and confirm the passphrase.
3. Create cluster peering on the source using the destination cluster LIF IP address as the `peer-addrs`. For HA pairs, list the destination intercluster LIF IP address for both nodes as the `-peer-addrs`.

   ```
   src::> cluster peer create -peer-addrs <10.161.189.18>
   ```

4. Enter and confirm the passphrase.
5. Check that the cluster peered.

```
src::> cluster peer show
```

Successful peering shows **Available** in the availability field.

6. Create SVM peering on the destination. Both source and destination SVMs should be data SVMs.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. Accept SVM peering.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. Check that the SVM peered.

```
dest::> vserver peer show
```

Peer state shows **`peered`** and peering applications shows **`snapmirror`**.

Step 5: Create a SnapMirror replication relationship between the source and destination system

This section provides instructions for how to create a SnapMirror replication relationship between the source and destination system.

To move an existing SnapMirror replication relationship, you must first break the existing SnapMirror replication relationship before you create a new SnapMirror replication relationship.

Use the ONTAP CLI for the following steps.

Steps

1. Create a data protected volume on the destination SVM.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. Create the SnapMirror replication relationship on the destination which includes the SnapMirror policy and schedule for the replication.

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. Initialize the SnapMirror replication relationship on the destination.

   ```
   dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
   ```

4. In the ONTAP CLI, validate the SnapMirror relationship status by running the following command:

   ```
   dest::> snapmirror show
   ```

   The relationship status is `Snapmirrored` and the health of the relationship is `true`.

5. Optional: In the ONTAP CLI, run the following command to view the actions history for the SnapMirror relationship.

   ```
   dest::> snapmirror show-history
   ```

Optionally, you can mount the source and destination volumes, write a file to the source, and verify the volume is replicating to the destination.

Google Cloud administration

Change the Google Cloud machine type for Cloud Volumes ONTAP

You can choose from several machine types when you launch Cloud Volumes ONTAP in Google Cloud. You can change the instance or machine type at any time if you determine that it is undersized or oversized for your needs.

About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn’t, then the operation will fail.

  ONTAP 9 Documentation: Commands for configuring automatic giveback

- Changing the machine type can affect Google Cloud service charges.
- The operation restarts Cloud Volumes ONTAP.

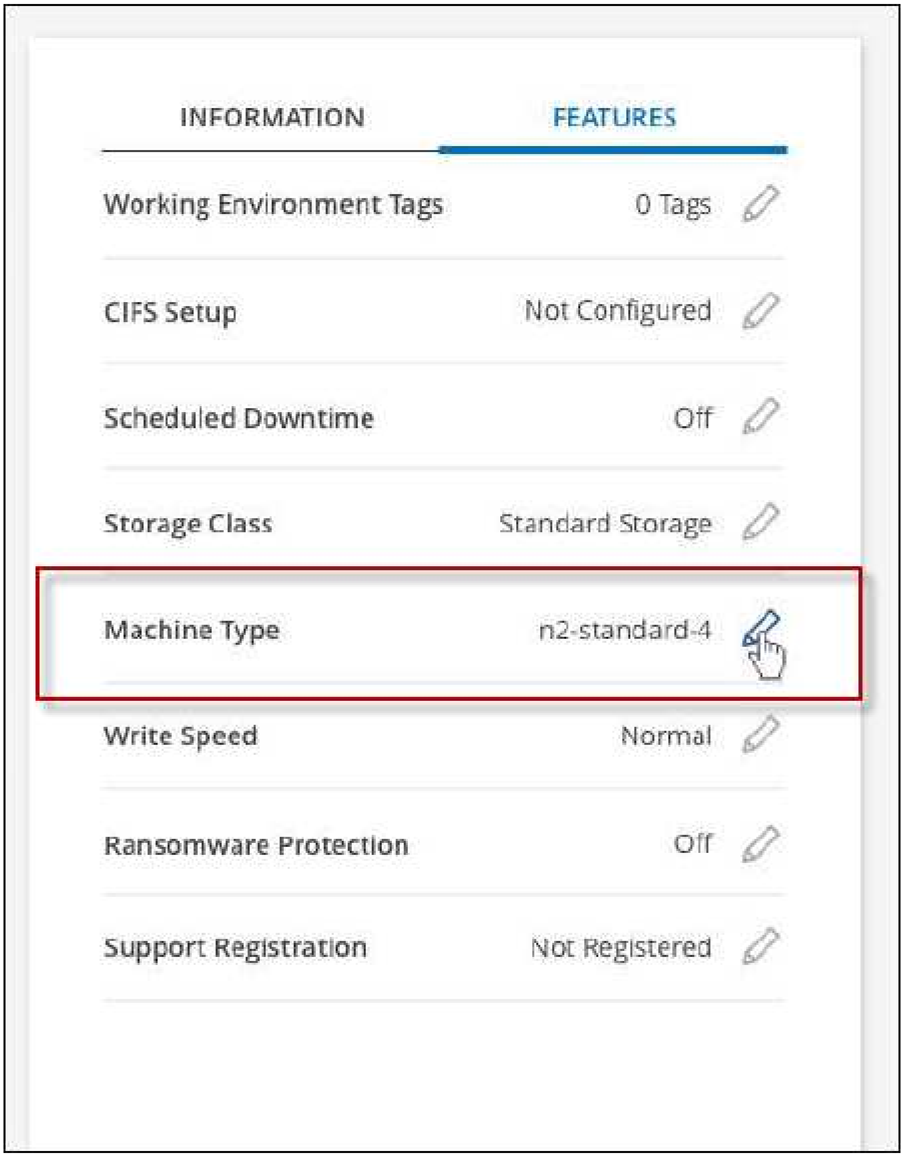
  For single node systems, I/O is interrupted.

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

  > 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 **Machine type**.



Working Environment Tags	0 Tags
CIFS Setup	Not Configured
Scheduled Downtime	Off
Storage Class	Standard Storage
Machine Type	n2-standard-4
Write Speed	Normal
Ransomware Protection	Off
Support Registration	Not Registered

If you are using a node-based pay-as-you-go (PAYGO) license, you can optionally choose a different license and machine type by clicking the pencil icon next to **License type**.

1. Choose an machine type, select the check box to confirm that you understand the implications of the change, and then click **Change**.

Result

Cloud Volumes ONTAP reboots with the new configuration.

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.

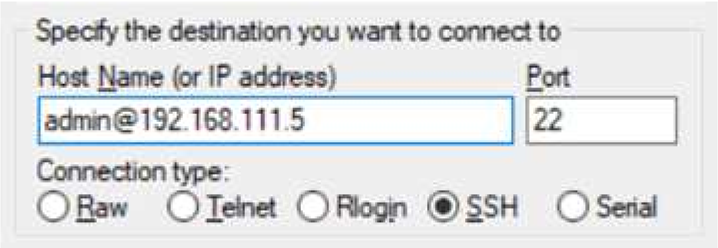
> When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

Steps

1. In 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:

   Specify the destination you want to connect to

   Host Name (or IP address): admin@192.168.111.5

   Port: 22

   Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

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

   Learn more about Connecting to the Linux VM for the Connector

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

   The basic structure of the file is as follows:

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

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

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

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

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

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

    ```
    http_access allow cvonet
    ```

    Here’s an example:

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

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

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

    ```
    docker restart squid
    ```

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

    ```
    autosupport check show-details
    ```

Configure EMS 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.

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.