System administration

Cloud Volumes ONTAP

NetApp
February 10, 2026

Table of Contents

System administration

Upgrade Cloud Volumes ONTAP

Upgrade Cloud Volumes ONTAP from the NetApp Console to gain access to the latest new features and enhancements. You should prepare Cloud Volumes ONTAP systems before you upgrade the software.

Upgrade overview

You should be aware of the following before you start the Cloud Volumes ONTAP upgrade process.

Upgrade from Console only

You should not upgrade Cloud Volumes ONTAP by using ONTAP System Manager or the ONTAP CLI, but only the Console. Otherwise, it might impact system stability.

The Console provides two ways to upgrade Cloud Volumes ONTAP:

- By following upgrade notifications that appear on the system
- By placing the upgrade image at an HTTPS location and then providing the Console with the URL

Supported upgrade paths

The Cloud Volumes ONTAP version you can upgrade to depends on the version you are currently running. Each generic or patch version in a release in the following tables represents the base version available for upgrade. For details about the available patches, refer to the versioned release notes for each release.

Supported upgrade paths for AWS

Current version	Versions that you can directly upgrade to
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0

Current version	Versions that you can directly upgrade to
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Supported upgrade paths for Azure

Current version	Versions that you can directly upgrade to
9.17.1 P1	9.18.1
9.16.1 P3	9.17.1 P1
9.15.1 P10	9.16.1 P3
9.14.1 P13	9.15.1 P10
9.13.1 P16	9.14.1 P13
9.12.1 P18	9.13.1 P16
9.11.1 P20	9.12.1 P18

If you have a lower version of Cloud Volumes ONTAP in Azure, you must first upgrade to the next version and follow the supported upgrade paths to reach your target version. For example, if you have Cloud Volumes ONTAP 9.7 P7, follow this upgrade path:

- 9.7 P7 → 9.8 P18
- 9.8 P18 → 9.9.1 P15
- 9.9.1 P15 → 9.10.1 P12
- 9.10.1 P12 → 9.11.1 P20

Supported upgrade paths for Google Cloud

Current version	Versions that you can directly upgrade to
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4

Current version	Versions that you can directly upgrade to
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Note the following:

- The supported upgrade paths for Cloud Volumes ONTAP are different than they are for an on-premises ONTAP cluster.
- If you upgrade by following the notifications that appear in a system, the Console will prompt you to upgrade to a release that follows these supported upgrade paths.
- If you upgrade by placing an upgrade image at an HTTPS location, be sure to follow these supported upgrade paths.
- In some cases, you might need to upgrade a few times to reach your target release.

  For example, if you're running version 9.8 and you want to upgrade to 9.10.1, you first need to upgrade to version 9.9.1 and then to 9.10.1.

Patch releases

Starting in January 2024, patch upgrades are only available if there's a patch release for the three latest versions of Cloud Volumes ONTAP. Patch versions are occasionally available for deployment, when the RC or GA version isn't available for deployment.

We use the latest GA release to determine the three latest versions to display in the Console. For example, if the current GA release is 9.13.1, patches for 9.11.1-9.13.1 appear in the Console.

For patch versions 9.11.1 or below, you will need to use a manual upgrade procedure by downloading the ONTAP image.

As a general rule for patch releases, you can upgrade from a lower patch version to any higher patch version in the same or the next Cloud Volumes ONTAP release.

Here are a couple of examples:

- 9.13.0 → 9.13.1 P15
- 9.12.1 → 9.13.1 P2

Reverting or downgrading

Reverting or downgrading Cloud Volumes ONTAP to a previous release is not supported.

Support registration

Cloud Volumes ONTAP must be registered with NetApp Support in order to upgrade the software using any of the methods described on this page. This applies to both pay-as-you-go (PAYGO) and bring your own license (BYOL). You'll need to manually register PAYGO systems, while BYOL systems are registered by default.

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

Upgrades of the HA mediator

The Console also updates the mediator instance as needed during the Cloud Volumes ONTAP upgrade process.

Upgrades in AWS with c4, m4, and r4 EC2 instance types

Cloud Volumes ONTAP no longer supports the c4, m4, and r4 EC2 instance types. You can upgrade existing deployments to Cloud Volumes ONTAP versions 9.8-9.12.1 with these instance types. Before you upgrade we recommend that you change the instance type. If you can't change the instance type, you need to enable enhanced networking before you upgrade. Read the following sections to learn more about changing the instance type and enabling enhanced networking.

In Cloud Volumes ONTAP running versions 9.13.0 and above, you cannot upgrade with c4, m4, and r4 EC2 instance types. In this case, you need to reduce the number of disks and then change the instance type or deploy a new HA-pair configuration with the c5, m5, and r5 EC2 instance types and migrate the data.

Change the instance type

c4, m4, and r4 EC2 instance types allow for more disks per node than the c5, m5, and r5 EC2 instance types. If the disk count per node for the c4, m4, or r4 EC2 instance you're running is below the max disk allowance per node for c5, m5, and r5 instances, you can change the EC2 instance type to c5, m5, or r5.

Check disk and tiering limits by EC2 instance
Change the EC2 instance type for Cloud Volumes ONTAP

If you can't change the instance type, follow the steps in Enable enhanced networking.

Enable enhanced networking

To upgrade to Cloud Volumes ONTAP versions 9.8 and later, you must enable *enhanced networking* on the cluster running the c4, m4, or r4 instance type. To enable ENA, refer to the Knowledge Base article "How to enable Enhanced networking like SR-IOV or ENA on AWS Cloud Volumes ONTAP instances".

Prepare to upgrade

Before performing an upgrade, you must verify that your systems are ready and make any required configuration changes.

- Plan for downtime
- Verify that automatic giveback is still enabled
- Suspend SnapMirror transfers
- Verify that aggregates are online
- Verify that all LIFs are on home ports

Plan for downtime

When you upgrade a single-node system, the upgrade process takes the system offline for up to 25 minutes,

during which I/O is interrupted.

In many cases, upgrading an HA pair is nondisruptive and I/O is uninterrupted. During this nondisruptive upgrade process, each node is upgraded in tandem to continue serving I/O to clients.

Session-oriented protocols might cause adverse effects on clients and applications in certain areas during upgrades. For details, refer to the ONTAP documentation

Verify that automatic giveback is still enabled

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

ONTAP documentation: Commands for configuring automatic giveback

Suspend SnapMirror transfers

If a Cloud Volumes ONTAP system has active SnapMirror relationships, it is best to suspend transfers before you update the Cloud Volumes ONTAP software. Suspending the transfers prevents SnapMirror failures. You must suspend the transfers from the destination system.

> Even though NetApp Backup and Recovery uses an implementation of SnapMirror to create backup files (called SnapMirror Cloud), backups do not need to be suspended when a system is upgraded.

About this task

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

Steps

1. Log in to System Manager from the destination system.

   You can log in to System Manager by pointing your web browser to the IP address of the cluster management LIF. You can find the IP address in the Cloud Volumes ONTAP system.

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

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

Verify that aggregates are online

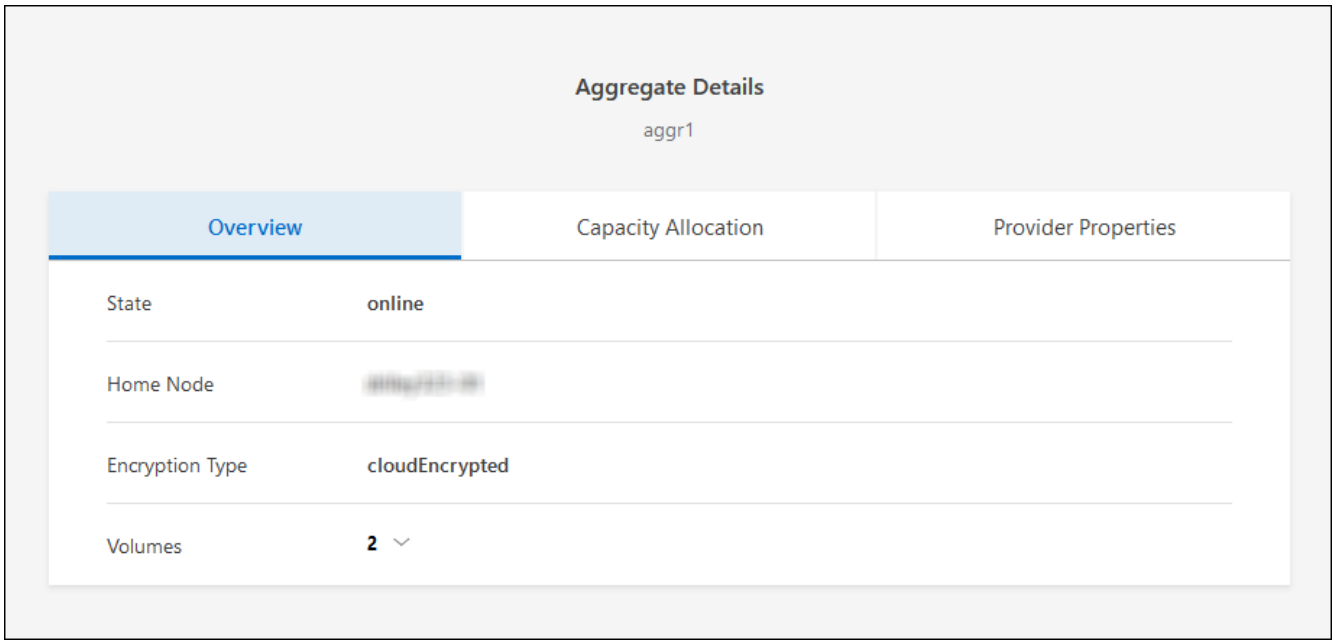
Aggregates for Cloud Volumes ONTAP must be online before you update the software. Aggregates should be online in most configurations, but if they are not, then you should bring them online.

About this task

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

Steps

1. On the Cloud Volumes ONTAP system, click the **Aggregates** tab.
2. On the required aggregate tile, click the ••• icon, and then select **View Aggregate details**.



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

Verify that all LIFs are on home ports

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

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

Upgrade Cloud Volumes ONTAP

The Console notifies you when a new version is available for upgrade. You can start the upgrade process from this notification. For more information, see Upgrade from Console notifications.

Another way to perform software upgrades by using an image on an external URL. This option is helpful if the Console can't access the S3 bucket to upgrade the software or if you were provided with a patch. For more information, see Upgrade from an image available at a URL.

Upgrade from Console notifications

The Console displays a notification in Cloud Volumes ONTAP working environments when a new version of Cloud Volumes ONTAP is available:

> Before you can upgrade Cloud Volumes ONTAP through the notifications, you must have a NetApp Support Site account.

You can start the upgrade process from this notification, which automates the process by obtaining the software image from an S3 bucket, installing the image, and then restarting the system.

Before you begin

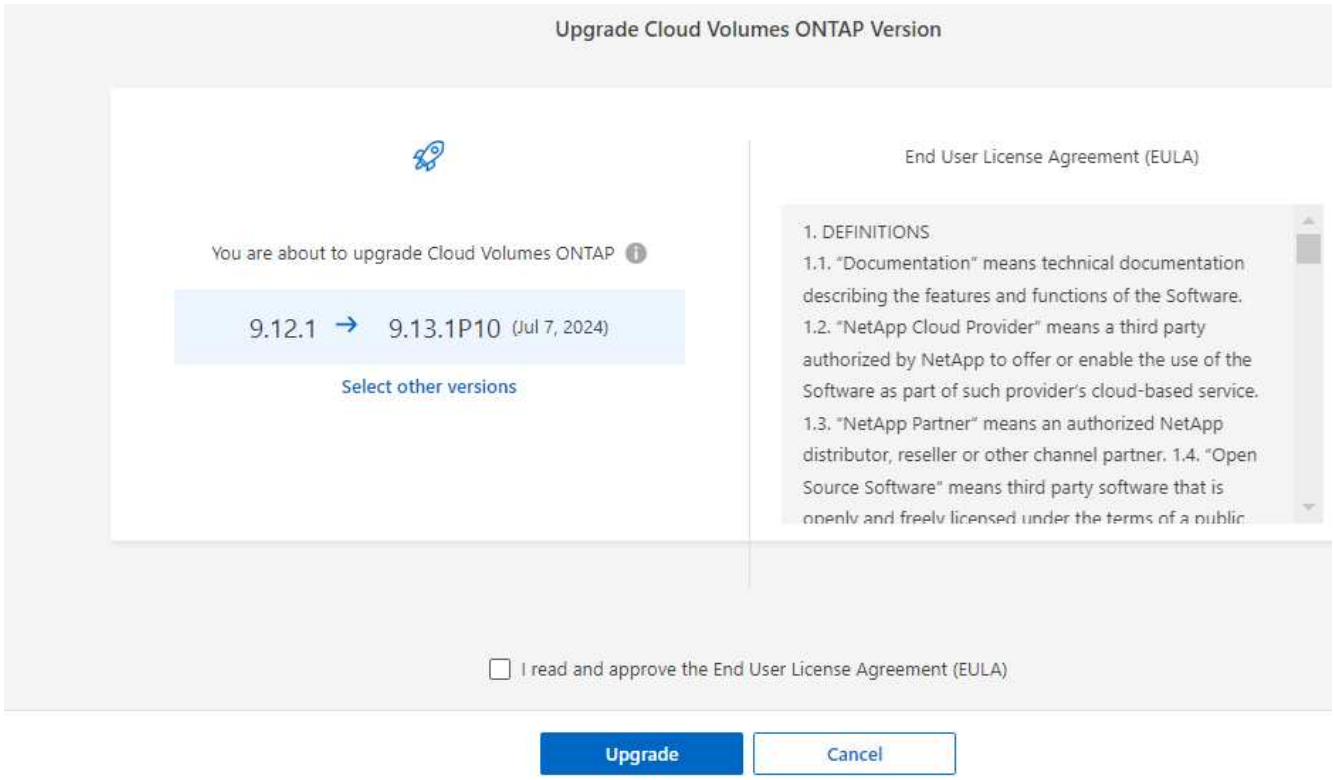
Operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. Select a Cloud Volumes ONTAP system.

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

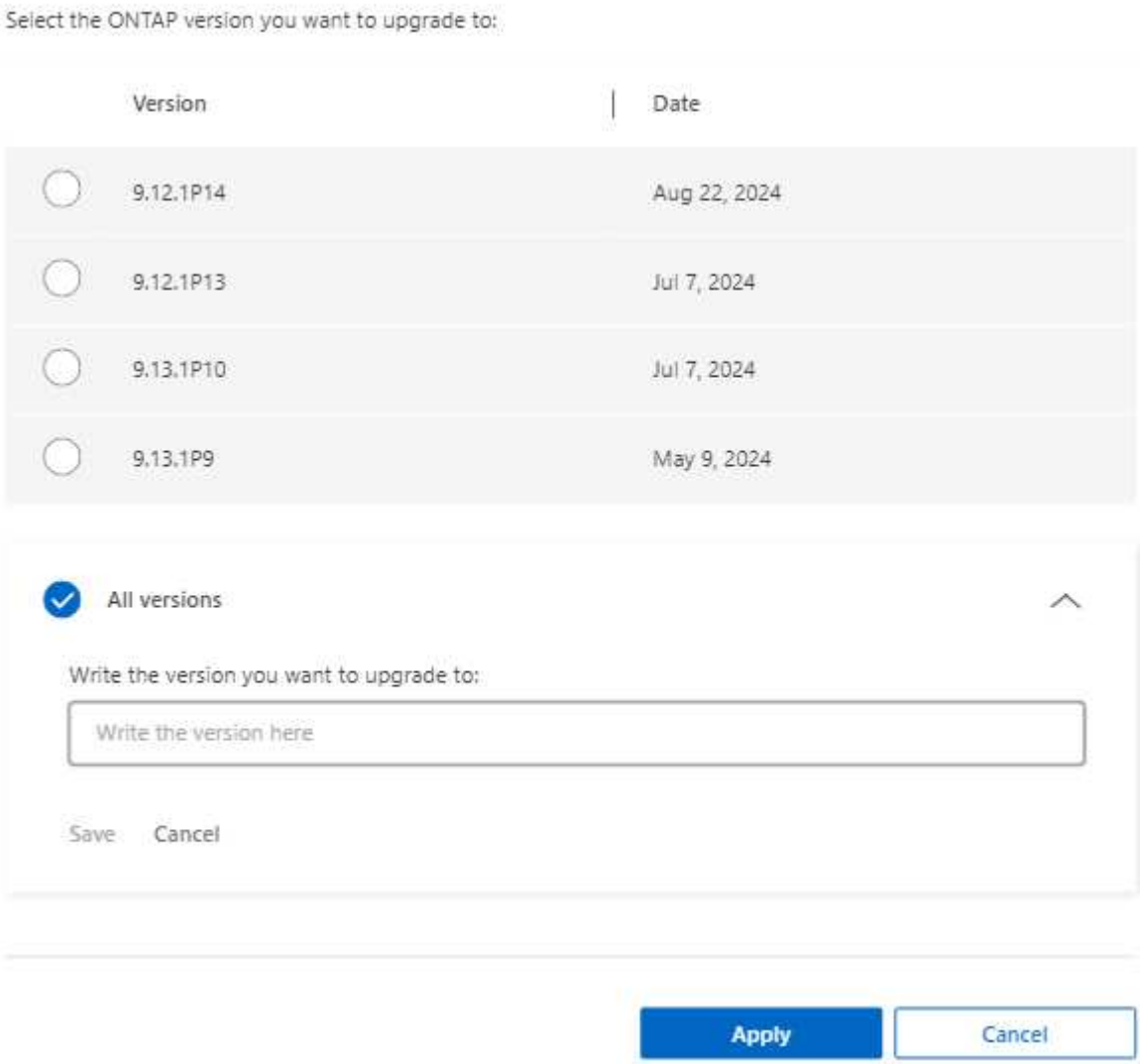
3. If you want to upgrade the installed version of Cloud Volumes ONTAP, click **Upgrade Now!** By default, you see the latest, compatible version for upgrade.



   If you want to upgrade to another version, click **Select other versions**. You see the latest Cloud Volumes ONTAP versions listed that are also compatible with the installed version on your system.
   For example, the installed version on your system is 9.12.1P3, and the following compatible versions are available:

- 9.12.1P4 to 9.12.1P14
- 9.13.1 and 9.13.1P1
  You see 9.13.1P1 as the default version for upgrade, and 9.12.1P13, 9.13.1P14, 9.13.1, and 9.13.1P1 as the other available versions.

4. Optionally, you can click **All versions** to enter another version that you want to upgrade to (say, the next patch of the installed version). For a compatible upgrade path of your current Cloud Volumes ONTAP version, refer to Supported upgrade paths.
5. Click **Save**, and then **Apply**.



6. In the Upgrade Cloud Volumes ONTAP page, read the EULA, and then select **I read and approve the EULA**.
7. Select **Upgrade**.
8. To view the progress, on the Cloud Volumes ONTAP system, select **Audit**.

Result

The Console starts the software upgrade. You can perform actions on the system when the software update is complete.

After you finish

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

Upgrade from an image available at a URL

You can place the Cloud Volumes ONTAP software image on the Console agent or on an HTTP server and then initiate the software upgrade from the Console. You might use this option if the Console can't access the S3 bucket to upgrade the software.

Before you begin

- Operations such as volume or aggregate creation must not be in progress on the Cloud Volumes ONTAP system.
- If you use HTTPS to host ONTAP images, the upgrade can fail due to SSL authentication issues, which are caused by missing certificates. The workaround is to generate and install a CA-signed certificate to be used for authentication between ONTAP and the Console.

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

  NetApp KB: How to configure the Console as an HTTPS server to host upgrade images

Steps

1. Optional: Set up an HTTP server that can host the Cloud Volumes ONTAP software image.

   If you have a VPN connection to the virtual network, you can place the Cloud Volumes ONTAP software image on an HTTP server in your own network. Otherwise, you must place the file on an HTTP server in the cloud.

2. If you use your own security group for Cloud Volumes ONTAP, ensure that the outbound rules allow HTTP connections so Cloud Volumes ONTAP can access the software image.

   The predefined Cloud Volumes ONTAP security group allows outbound HTTP connections by default.

3. Obtain the software image from the NetApp Support Site.
4. Copy the software image to a directory on the Console agent or on an HTTP server from which the file will be served.

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

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

5. On the system, click the ••• icon, and then click **Update Cloud Volumes ONTAP**.
6. On the Update Cloud Volumes ONTAP version page, enter the URL, and then click **Change Image**.

   If you copied the software image to the Console agent in the path shown above, you would enter the following URL:

   http://<Console_agent_private-IP-address>/ontap/images/<image-file-name>

   In the URL, **image-file-name** must follow the format "cot.image.9.13.1P2.tgz".

7. Click **Proceed** to confirm.

Result

The Console starts the software update. You can perform actions on the system once the software update is complete.

After you finish

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

Fix download failures when using a Google Cloud NAT gateway

The Console agent automatically downloads software updates for Cloud Volumes ONTAP. The download can fail if your configuration uses a Google Cloud NAT gateway. You can correct this issue by limiting the number of parts that the software image is divided into. You must use the APIs to complete this step.

Step

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

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

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

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

Learn more about the /occm/config API call.

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

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

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

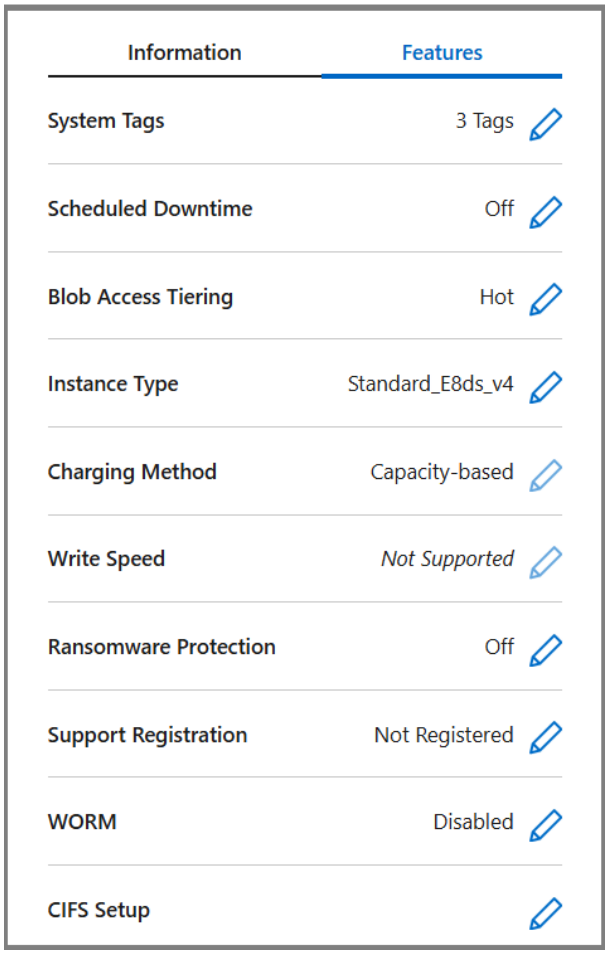
A system that isn't registered for support will still receive the software update notifications that appear in the NetApp Console when a new version is available. But you will need to register the system before you can upgrade the software.

Steps

1. If you have not yet added your NetApp Support Site account to the Console, go to **Account Settings** and add it now.

   Learn how to add NetApp Support Site accounts.

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



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

Result

The system is registered with NetApp.

Convert a Cloud Volumes ONTAP node-based license to a capacity-based license

After the end of availability (EOA) of your node-based licenses, you should transition to capacity-based licensing by using the license conversion tool in the NetApp Console.

For annual or longer-term commitments, NetApp recommends that you contact your NetApp representative prior to the EOA date (11 November, 2024) or license expiration date to ensure that the prerequisites for the transition are in place. If you don't have a long-term contract for a Cloud Volumes ONTAP node and run your system against an on-demand pay-as-you-go (PAYGO) subscription, it is important to plan your conversion before the end of support (EOS) on 31 December, 2024. In both the cases, you should ensure that your system fulfills the requirements before you use the license conversion tool in the NetApp Console for a seamless transition.

For information about the EOA and EOS, refer to End of availability of node-based licenses.

About this task

- When you use the license conversion tool, the transition from node-based to capacity-based licensing model is carried out in place and online that eliminates the need for any data migration or provisioning of

additional cloud resources.

- It is a non-disruptive operation, and no service disruption or application downtime occurs.
- The account and application data in your Cloud Volumes ONTAP system remains intact.
- The underlying cloud resources remain unaffected post conversion.
- The license conversion tool supports all deployment types, such as single node, high availability (HA) in single availability zone (AZ), HA in multiple AZ, bring your own license (BYOL), and PAYGO.
- The tool supports all node-based licenses as the source and all capacity-based licenses as the destination. For example, if you have a PAYGO Standard node-based license, you can convert it to any capacity-based license purchased through the marketplace. NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP.
- The conversion is supported for all cloud providers, AWS, Azure, and Google Cloud.
- Post conversion, the serial number of the node-based license will be replaced by a capacity-based format. This is done as a part of the conversion, and is reflected on your NetApp Support Site (NSS) account.
- When you transition to the capacity-based model, your data continues to be retained in the same location as the node-based licensing. This approach guarantees no disruption in data placement, and upholds data sovereignty principles throughout the transition.

Before your begin

- You should have an NSS account with customer access or administrator access.
- Your NSS account should be registered with the user credentials you used for accessing the Console.
- The Cloud Volumes ONTAP system should be linked to the NSS account with customer access or administrator access.
- You should have a valid capacity-based license in place, either a BYOL license or marketplace subscription.
- A capacity-based license should be available in your account. This license can be a marketplace subscription or a BYOL/private offer package available under **Licenses and subscriptions** in the Console.
- Understand the following criteria before selecting a destination package:
  - If the account has a capacity-based BYOL license, the destination package selected should align with the account's BYOL capacity-based licenses:
    - When `Professional` is selected as the destination package, the account should have a BYOL license with a Professional package:
    - When `Essentials` is selected as the destination package, the account should have a BYOL license with the Essentials package.
  - If the destination package does not align with the account's BYOL license availability, it implies that the capacity-based license might not include the selected package. In this case, you will be charged through your marketplace subscription.
  - If there is no capacity-based BYOL license but only a marketplace subscription, you should ensure that the selected package is included in your capacity-based marketplace subscription.
  - If there is not enough capacity in your existing capacity-based license, and if you have a marketplace subscription to charge for the additional capacity usage, you will be charged for the additional capacity through your marketplace subscription.
  - If there is not enough capacity in your existing capacity-based license, and you don't have a marketplace subscription to charge for the additional capacity usage, the conversion cannot occur. You should add a marketplace subscription to charge the additional capacity or extend the available

capacity to your current license.

- If the destination package does not align with the account's BYOL license availability and also if there is not enough capacity in your existing capacity-based license, then you will be charged through your marketplace subscription.

If any of these requirements is not fulfilled, the license conversion does not happen. In specific cases, the license might be converted, but cannot be used. Click the information icon to identify the issues and take corrective actions.

Steps

1. On the **Systems** page, double-click the name of the system for which you want to modify the license type.
2. On the Overview tab, click the Features panel.
3. Check the pencil icon next to **Charging method**. If the charging method for your system is `Node Based`, you can convert it to by-capacity charging.

   The icon is disabled if your Cloud Volumes ONTAP system is already charged by capacity, or if any of the requirements is not fulfilled.

4. On the **Convert Node-based licenses to Capacity-based** screen, verify the system name and source license details.
5. Select the destination package for converting the existing license:
   - Essentials. The default value is `Essentials`.
   - Professional
6. If you have a BYOL license, you can select the checkbox to delete the node-based license from the Console after the conversion is complete. If the conversion is still in progress, selecting this checkbox will not remove the license from the Console. This option is not available for marketplace subscriptions.
7. Select the check box to confirm that you understand the implications of the change, and then click **Proceed**.

After you finish

View the new license serial number and verify the changes in the **Licenses and subscriptions** menu of the Console.

Pricing in different hyperscalars

For details on pricing, go to the NetApp Console website.

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

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

Start and stop a Cloud Volumes ONTAP system

You can stop and start Cloud Volumes ONTAP from the NetApp Console to manage your cloud compute costs.

Scheduling automatic shutdowns of Cloud Volumes ONTAP

You might want to shut down Cloud Volumes ONTAP during specific time intervals to lower your compute costs. Rather than do this manually, you can configure the Console to automatically shut down and then restart systems at specific times.

About this task

- When you schedule an automatic shutdown of your Cloud Volumes ONTAP system, the Console postpones the shutdown if an active data transfer is in progress.

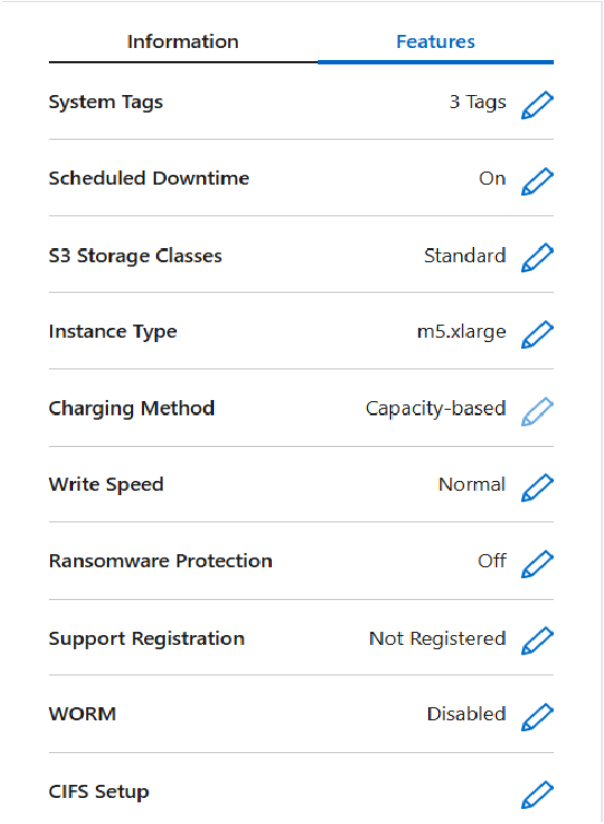
  It shuts down the system after the transfer is complete.

- This task schedules automatic shutdowns of both nodes in an HA pair.
- Snapshots of boot and root disks are not created when turning off Cloud Volumes ONTAP through scheduled shutdowns.

  Snapshots are automatically created only when performing a manual shutdown, as described in the next section.

Steps

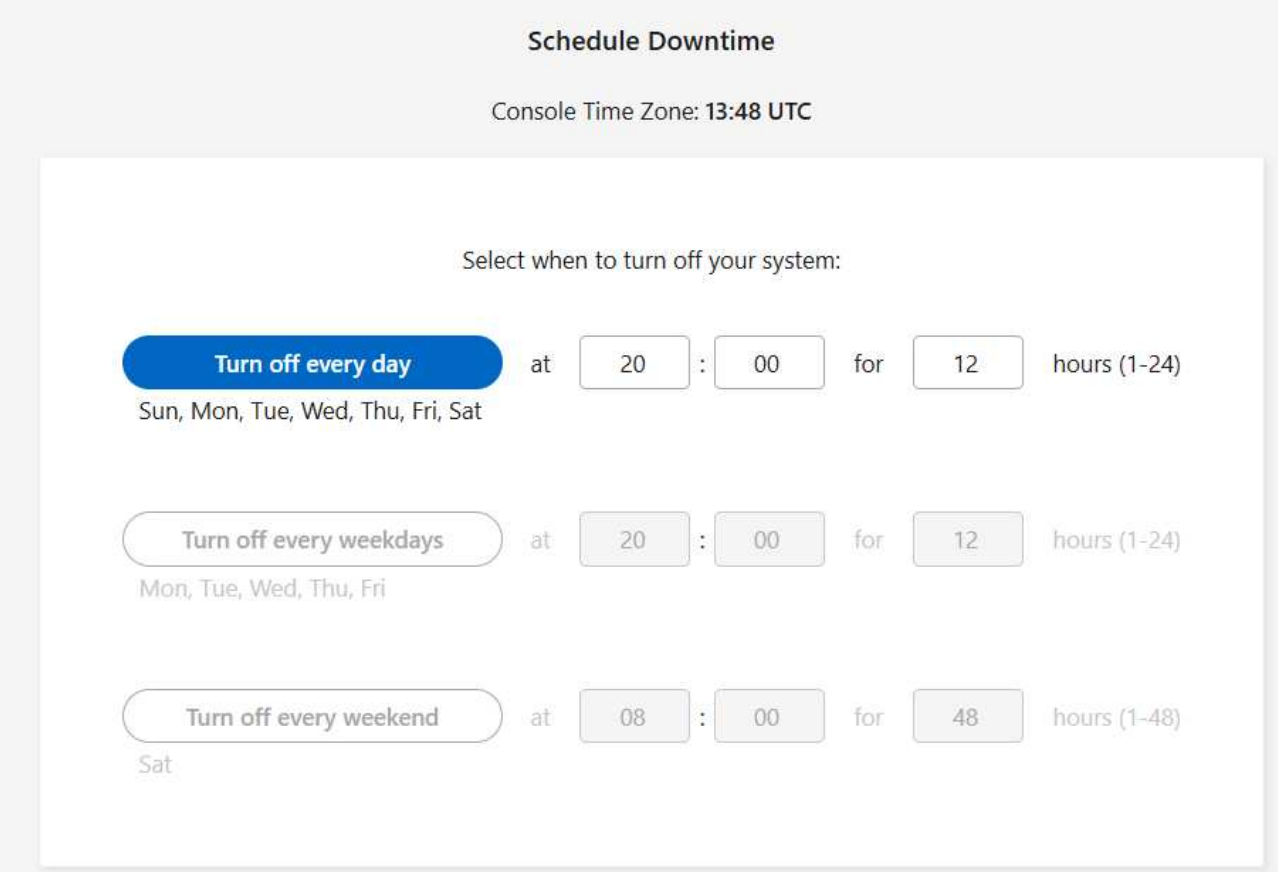
1. On the **Systems** page, double-click the Cloud Volumes ONTAP system.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Scheduled Downtime**.



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

Example

The following image shows a schedule that instructs the Console to shut down the system every Saturday at 20:00 P.M. (8:00 PM) for 12 hours. The Console restarts the system every Monday at 12:00 a.m.



4. Click **Save**.

Result

The schedule is saved. The corresponding Scheduled Downtime line item under the Features panel displays 'On'.

Stopping Cloud Volumes ONTAP

Stopping Cloud Volumes ONTAP saves you from accruing compute costs and creates snapshots of the root and boot disks, which can be helpful for troubleshooting.

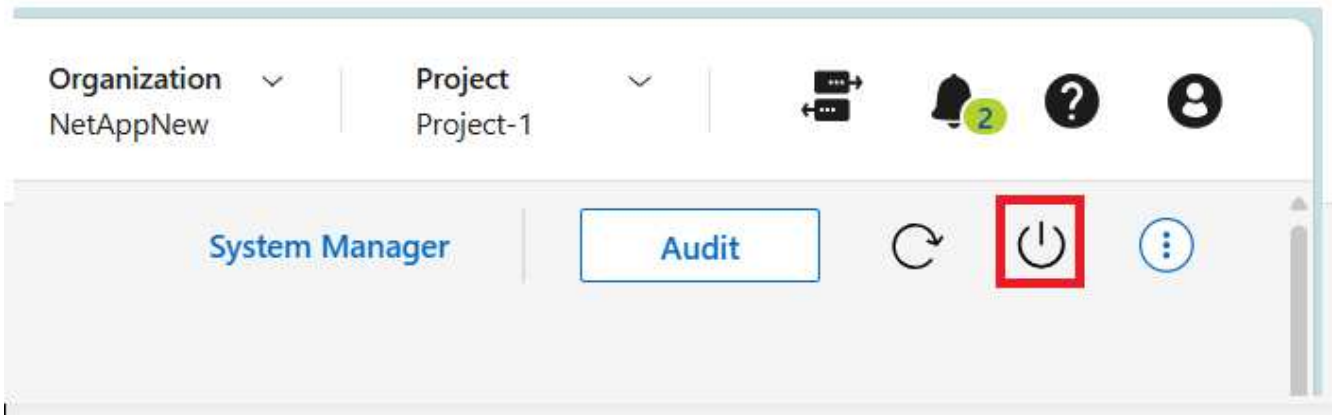
To reduce costs, the Console periodically deletes older snapshots of root and boot disks. Only the two most recent snapshots are retained for both the root and boot disks.

About this task

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

Steps

1. From the system, click the **Turn off** icon.



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

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

   Snapshots are created automatically upon reboot.

Synchronize Cloud Volumes ONTAP system time using the NTP server

To ensure accurate time synchronization, you must set up a Network Time Protocol (NTP) server for your Cloud Volumes ONTAP systems. Make sure to configure an NTP server for your Cloud Volumes ONTAP systems on all cloud providers to maintain consistent time synchronization within your network.

If you don't configure an NTP server, you might experience service disruptions and inaccurate time synchronization.

You can specify an NTP server using:

- The NetApp Console API.
- The ONTAP CLI command cluster time-service ntp server create.

Related links

- Knowledge base (KB) article: How does a CVO cluster use NTP?
- Prepare to use the API
- Cloud Volumes ONTAP workflows
- Get required identifiers
- Use the REST APIs for NetApp Console

Modify system write speed

You can choose a normal or high write speed for Cloud Volumes ONTAP in the NetApp

Console. The default write speed is normal. You can change to high write speed if fast write performance is required for your workload.

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

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

About this task

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

Steps

1. On the **Systems** page, double-click the name of the system you configure to the write speed.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Write Speed**.
3. Select **Normal** or **High**.

   If you choose High, then you'll need to read the "I understand…" statement and confirm by checking the box.

   The **High** write speed option is supported with Cloud Volumes ONTAP HA pairs in Google Cloud starting with version 9.13.0.

4. Click **Save**, review the confirmation message, and then click **Approve**.

Change the Cloud Volumes ONTAP cluster admin password

Cloud Volumes ONTAP includes a cluster admin account. You can change the password for this account from NetApp Console, if needed.

You should not change the password for the admin account through ONTAP System Manager or the ONTAP CLI. The password will not be reflected in the Console. As a result, the Console cannot monitor the instance properly.

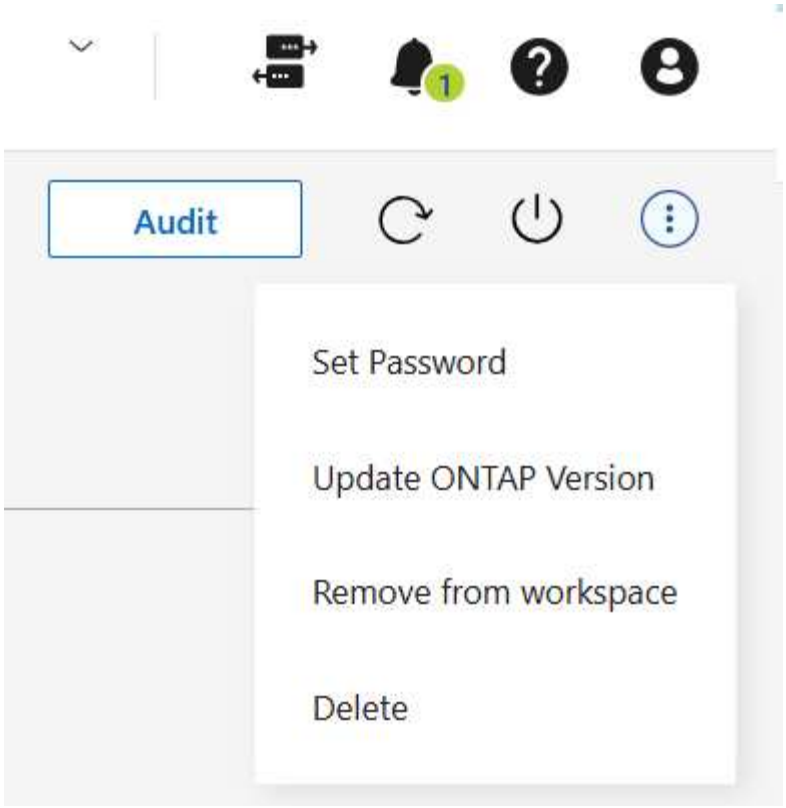
About this task

The password must observe a few rules. The new password:

- Shouldn't contain the word `admin`
- Must be between eight and 50 characters in length
- Must contain at least one English letter and one digit
- Shouldn't contain these special characters: `/ ( ) { } [ ] # : % " ? \`

Steps

1. On the **Systems** page, double-click the name of the Cloud Volumes ONTAP system.
2. On the upper right of the Console, click the ••• icon, and select **Set password**.



Add, remove, or delete systems

Add an existing Cloud Volumes ONTAP system to NetApp Console

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

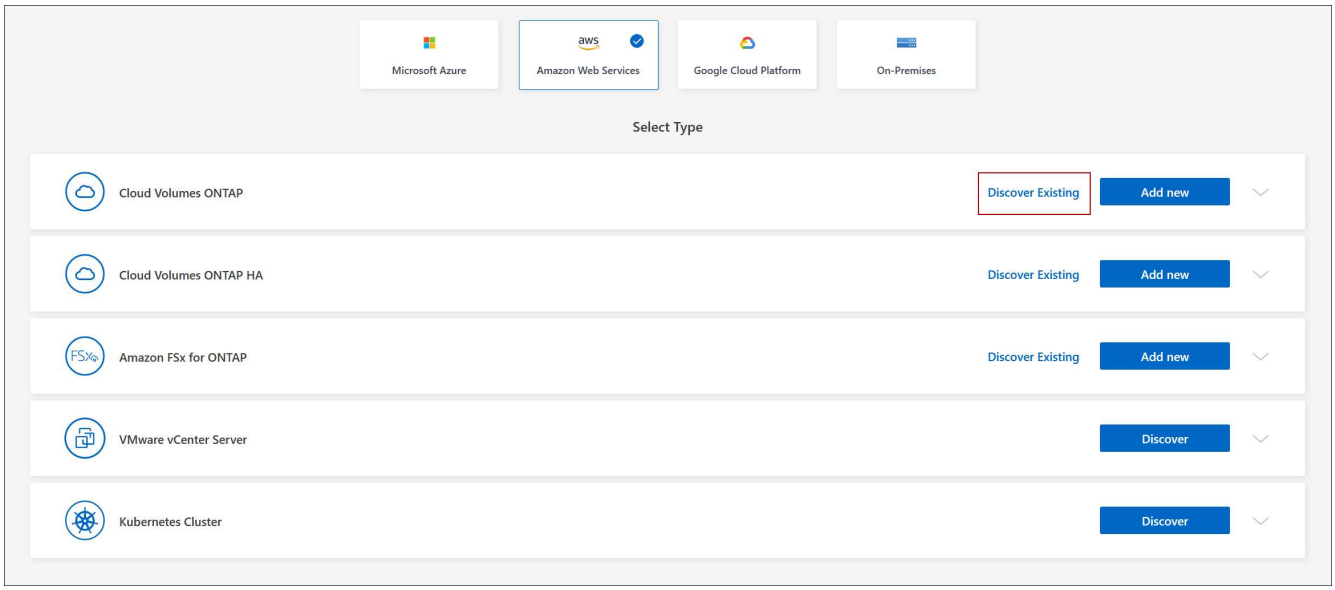
> You can only add systems that are registered with the account you used to log in to the Console. If you have multiple accounts or organizations, ensure that you are logged in to the correct account before adding systems. You can't discover, view, or manage systems that are registered with a different account or organization.

Before you begin

You must know the password for the Cloud Volumes ONTAP admin user account.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **System** page, click **Add System**.
3. Select the cloud provider in which the system resides.
4. Choose the type of Cloud Volumes ONTAP system to add.
5. Click the link to discover an existing system.



6. On the Region page, select a region. You can see the systems that are running in the selected region.

   Cloud Volumes ONTAP systems are represented as instances on this page. From the list, you can select only those instances that are registered with the current account.

7. On the Credentials page, enter the password for the Cloud Volumes ONTAP admin user, and then select **Go**.

Result

The Console adds the Cloud Volumes ONTAP systems to the **Systems** page.

Remove a Cloud Volumes ONTAP system from NetApp Console

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

About this task

Removing a Cloud Volumes ONTAP system removes it from the NetApp Console. It does not delete the Cloud Volumes ONTAP system. You can later rediscover the system if you need.

Steps

1. On the **Systems** page, double-click on the system you want to remove.
2. On the upper right of the Console, click the ••• icon, and select **Remove from workspace**.
3. In the **Remove from workspace** window, click **Remove**.

Result

The Console removes the system. Users can rediscover the deleted system from the **Systems** page at any time.

Delete a Cloud Volumes ONTAP system from NetApp Console

You should always delete Cloud Volumes ONTAP systems from the NetApp Console, rather than from your cloud provider's application. For example, if you terminate a

licensed Cloud Volumes ONTAP instance from your cloud provider, then you can't use the license key for another instance. You must delete the Cloud Volumes ONTAP system from the Console to release the license.

When you delete a system, the Console terminates Cloud Volumes ONTAP instances and deletes disks and snapshots.

> Other resources, such as backups managed by NetApp Backup and Recovery, and instances for NetApp Data Classification, are not deleted when you delete a system. You'll need to manually delete them. If you don't, then you'll continue to incur charges for these resources.

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

Steps

1. If you enabled Backup and Recovery on the system, determine whether the backed up data is still required and then delete the backups, if necessary.

   Backup and Recovery is independent from Cloud Volumes ONTAP by design. Backup and Recovery doesn't automatically delete backups when you delete a Cloud Volumes ONTAP system, and there is no current support in the UI to delete the backups after the system has been deleted.

2. If you enabled Data Classification on this system and no other systems use this service, then you need to delete the instance for the service.

   Learn more about the Data Classification instance.

3. Delete the Cloud Volumes ONTAP system.
   a. On the **Systems** page, double-click the name of the Cloud Volumes ONTAP system that you want to delete.
   b. On the upper right of the Console, click the ••• icon, and select **Delete**.
   c. Type the name of the system you want to delete, and then click **Delete**. It can take up to five minutes to delete a system.

> Backup and Recovery is free only for Cloud Volumes ONTAP Professional licenses. This free benefit does not apply to deleted environments. If backed up copies of the Cloud Volumes ONTAP environment are retained in a Backup and Recovery instance, you will be charged for the backed up copies until they are deleted.

AWS administration

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

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

About this task

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

ONTAP 9 Documentation: Commands for configuring automatic giveback

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

  For single node systems, I/O is interrupted.

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

> The NetApp Console changes one node at a time by initiating takeover and waiting for give back. NetApp's Quality Assurance team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, some retries were observed on the I/O level, but the application layer overcame the rewiring of NFS/CIFS connections.

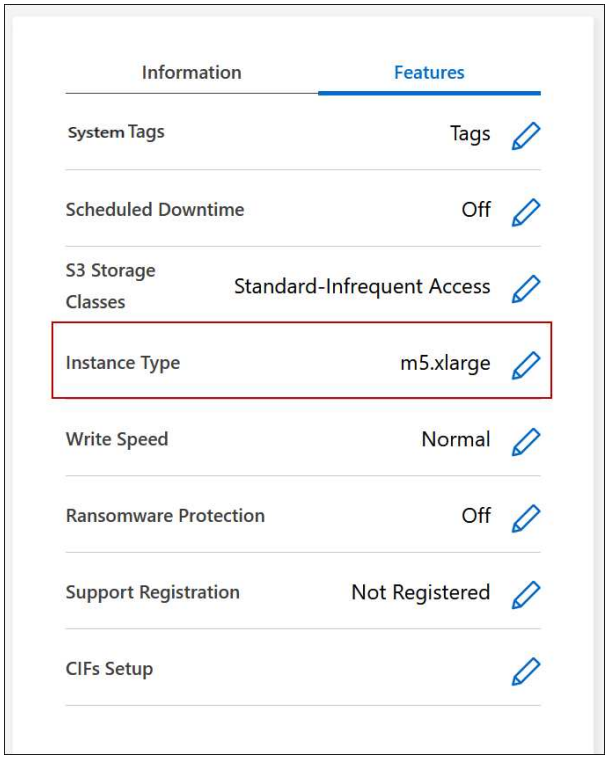
Reference

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

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

Steps

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



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

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

Result

Cloud Volumes ONTAP reboots with the new configuration.

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

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

Steps

1. On the **Systems** page, select the system.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Route tables**.
3. Modify the list of selected route tables and then click **Save**.

Result

The NetApp Console sends an AWS request to modify the route tables.

Azure administration

Change the Azure VM type for Cloud Volumes ONTAP

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

About this task

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

  ONTAP 9 Documentation: Commands for configuring automatic giveback

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

  For single node systems, I/O is interrupted.

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

  NetApp Console changes one node at a time by initiating takeover and waiting for give back. NetApp's Quality Assurance team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, some retries were observed on the I/O level, but the application layer overcame the rewiring of NFS/CIFS connections.

Steps

1. On the **Systems** page, select the system.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **VM type**.

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

3. Select a VM type, select the check box to confirm that you understand the implications of the change, and then click **Change**.

Result

Cloud Volumes ONTAP reboots with the new configuration.

Override CIFS locks for Cloud Volumes ONTAP HA pairs in Azure

The organization or account admin can enable a setting in the NetApp Console that prevents issues with Cloud Volumes ONTAP storage giveback during Azure maintenance events. When you enable this setting, Cloud Volumes ONTAP vetoes CIFS locks and resets active CIFS sessions.

About this task

Microsoft Azure schedules periodic maintenance events on its virtual machines. When a maintenance event occurs on a Cloud Volumes ONTAP HA pair, the HA pair initiates storage takeover. If there are active CIFS sessions during this maintenance event, the locks on CIFS files can prevent storage giveback.

If you enable this setting, Cloud Volumes ONTAP will veto the locks and reset the active CIFS sessions. As a result, the HA pair can complete storage giveback during these maintenance events.

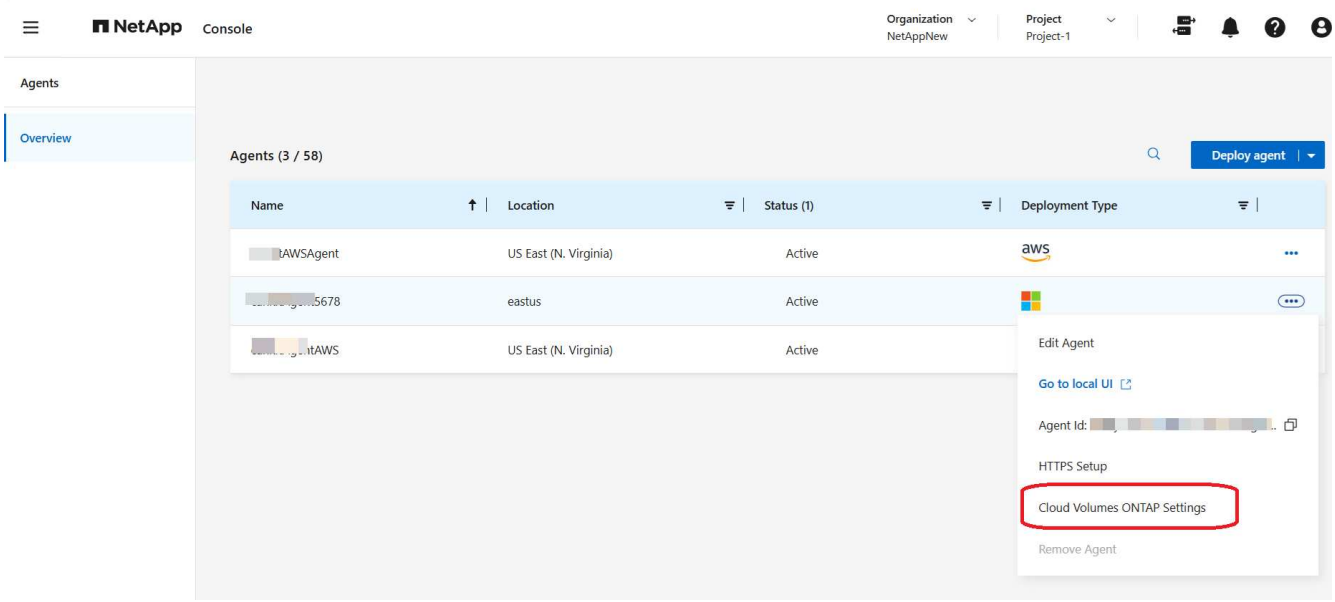
This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

Before you begin

You need to create a Console agent before you can change the Console settings. Learn how.

Steps

1. From the left navigation pane, go to **Administration > Agents**.
2. Click the ••• icon for the Console agent that manages your Cloud Volumes ONTAP system.
3. Select **Cloud Volumes ONTAP Settings**.



4. Under **Azure**, click **Azure CIFS locks for Azure HA systems**.
5. Click the checkbox to enable the feature and then click **Save**.

Use an Azure Private Link or service endpoints for Cloud Volumes ONTAP systems

Cloud Volumes ONTAP uses an Azure Private Link for connections to its associated storage accounts. If needed, you can disable Azure Private Links and use service endpoints instead.

Overview

By default, the NetApp Console enables an Azure Private Link for connections between Cloud Volumes ONTAP and its associated storage accounts. An Azure Private Link secures connections between endpoints in Azure and provides performance benefits.

If required, you can configure Cloud Volumes ONTAP to use service endpoints instead of an Azure Private Link.

With either configuration, the Console always limits network access for connections between Cloud Volumes ONTAP and storage accounts. Network access is limited to the VNet where Cloud Volumes ONTAP is deployed and the VNet where the Console agent is deployed.

Disable Azure Private Links and use service endpoints instead

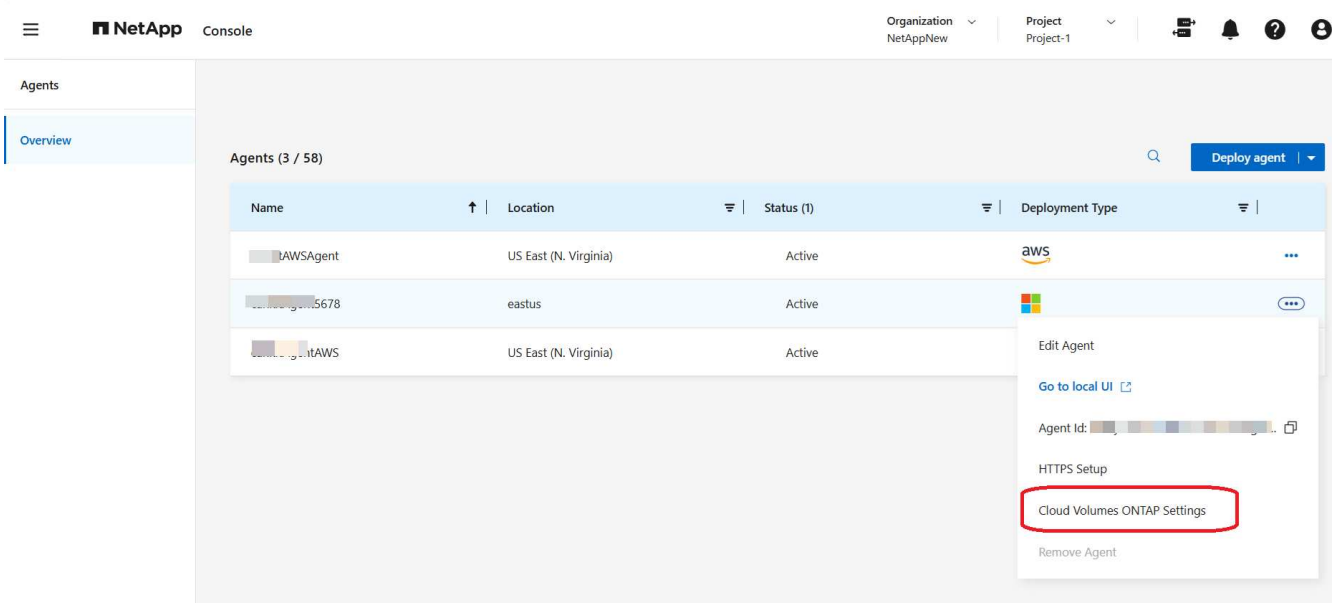
If required by your business, you can change a setting in the Console so that it configures Cloud Volumes ONTAP to use service endpoints instead of an Azure Private Link. Changing this setting applies to new Cloud Volumes ONTAP systems that you create. Service endpoints are only supported in Azure region pairs between the Console agent and Cloud Volumes ONTAP VNets.

The Console agent should be deployed in the same Azure region as the Cloud Volumes ONTAP systems that it manages, or in the Azure region pair for the Cloud Volumes ONTAP systems.

Steps

1. From the left navigation pane, go to **Administration > Agents**.

2. Click the ••• icon for the Console agent that manages your Cloud Volumes ONTAP system.
3. Select **Cloud Volumes ONTAP Settings**.



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

After you finish

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

Learn how to enable direct API traffic on the Console agent

Work with Azure Private Links

In most cases, there's nothing that you need to do to set up Azure Private links with Cloud Volumes ONTAP. The Console manages Azure Private Links for you. But if you use an existing Azure Private DNS zone, then you'll need to edit a configuration file.

Requirement for custom DNS

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

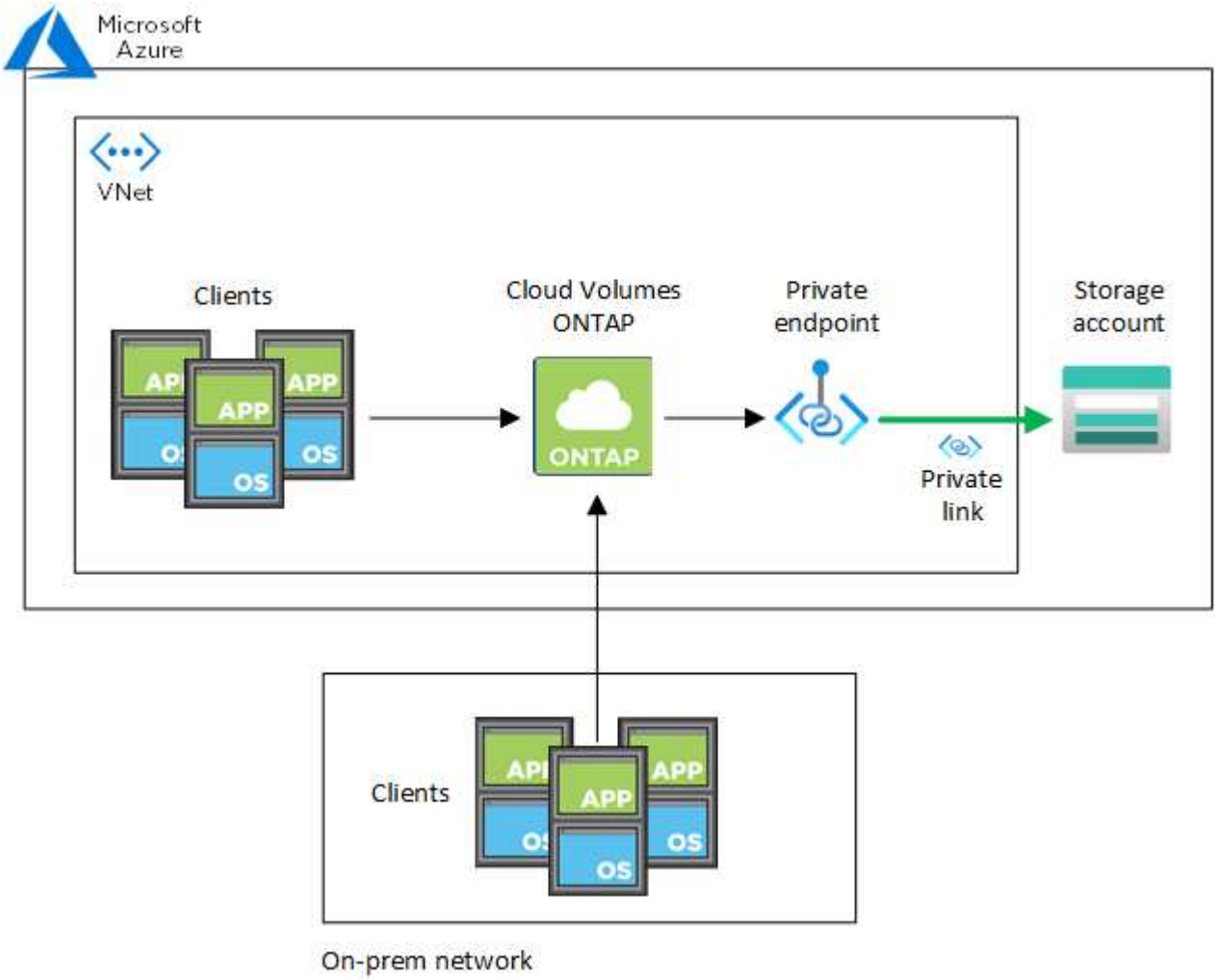
How Private Link connections work

When the Console deploys Cloud Volumes ONTAP in Azure, it creates a private endpoint in the resource group. The private endpoint is associated with storage accounts for Cloud Volumes ONTAP. As a result, access to Cloud Volumes ONTAP storage travels through the Microsoft backbone network.

Client access goes through the private link when clients are within the same VNet as Cloud Volumes ONTAP, within peered VNets, or in your on-premises network when using a private VPN or ExpressRoute connection to the VNet.

Here's an example that shows client access over a private link from within the same VNet and from an on-

premises network that has either a private VPN or ExpressRoute connection.



If the Console agent and Cloud Volumes ONTAP systems are deployed in different VNets, then you must set up VNet peering between the VNet where the Console agent is deployed and the VNet where the Cloud Volumes ONTAP systems are deployed.

Provide details about your Azure Private DNS

If you use Azure Private DNS, then you need to modify a configuration file on each Console agent. Otherwise, the Console can't set the Azure Private Link connection between Cloud Volumes ONTAP and its associated storage accounts.

Note that the DNS name must match Azure DNS naming requirements as shown in Azure documentation.

Steps

1. SSH to the Console agent host and log in.
2. Navigate to the `/opt/application/netapp/cloudmanager/docker_occm/data` directory.
3. Edit `app.conf` by adding the `user-private-dns-zone-settings` parameter with the following keyword-value pairs:

```
"user-private-dns-zone-settings" : {
   "resource-group" : "<resource group name of the DNS zone>",
   "subscription" : "<subscription ID>",
   "use-existing" : true,
   "create-private-dns-zone-link" : true
}
```

The `subscription` keyword is required only if the private DNS zone is in a different subscription than that of the Console agent.

4. Save the file and log off the Console agent.

   A reboot isn't required.

Enable rollback on failures

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

You can change this default behavior by enabling rollback if the Console fails to create the Azure Private Link. This can help to ensure that you're fully compliant with your company's security regulations.

If you enable rollback, the Console stops the action and rolls back all resources that were created as part of the action.

You can enable rollback through the API or by updating the app.conf file.

Enable rollback through the API

Step

1. Use the `PUT /occm/config` API call with the following request body:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

Enable rollback by updating app.conf

Steps

1. SSH to the host of the Console agent and log in.
2. Navigate to the following directory: /opt/application/netapp/cloudmanager/docker_occm/data
3. Edit app.conf by adding the following parameter and value:

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

4. Save the file and log off the Console agent.

A reboot isn’t required.

Move an Azure resource group for Cloud Volumes ONTAP in Azure console

Cloud Volumes ONTAP supports Azure resource groups moves but the workflow happens in the Azure console only.

You can move a Cloud Volumes ONTAP system from one resource group to a different resource group in Azure within the same Azure subscription. Moving resource groups between different Azure subscriptions is not supported.

Steps

1. Remove the Cloud Volumes ONTAP system. Refer to Removing Cloud Volumes ONTAP systems.
2. Execute the resource group move in the Azure console.

   To complete the move, refer to Move resources to a new resource group or subscription in Microsoft Azure’s documentation.

3. On the **Systems** page, discover the system.
4. Look for the new resource group in the information for the system.

Result

The system and its resources (VMs, disks, storage accounts, network interfaces, snapshots) are in the new resource group.

Segregate SnapMirror traffic in Azure

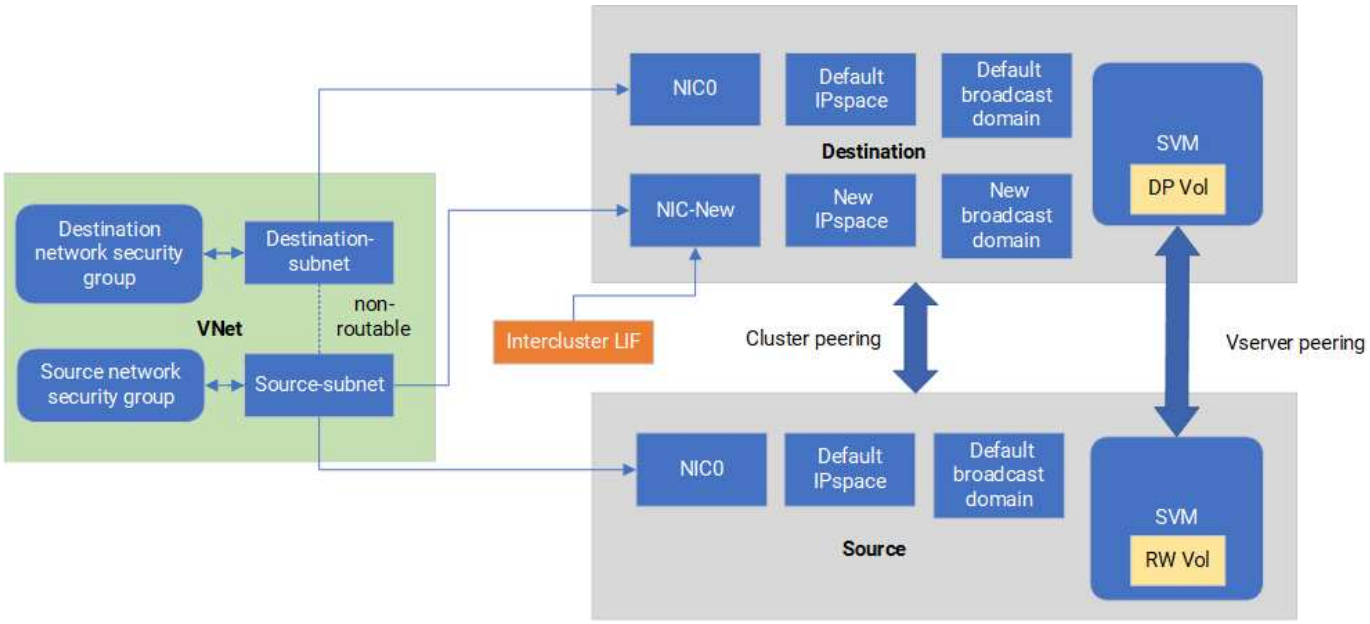
With Cloud Volumes ONTAP in Azure, you can segregate SnapMirror replication traffic from data and management traffic. To segregate SnapMirror replication traffic from your data traffic, you’ll add a new network interface card (NIC), an associated intercluster LIF and a non-routable subnet.

About SnapMirror traffic segregation in Azure

By default, the NetApp Console configures all NICs and LIFs in a Cloud Volumes ONTAP deployment on the same subnet. In such configurations, SnapMirror replication traffic and data and management traffic use the same subnet. Segregating SnapMirror traffic leverages an additional subnet that isn’t routable to the existing subnet used for data and management traffic.

Figure 1

The following diagrams show the segregation of SnapMirror replication traffic with an additional NIC, an associated intercluster LIF and a non-routable subnet in a single node deployment. An HA pair deployment differs slightly.



Before you begin

Review the following considerations:

- You can only add a single NIC to a Cloud Volumes ONTAP single node or HA-pair deployment (VM instance) for SnapMirror traffic segregation.
- To add a new NIC, the VM instance type you deploy must have an unused NIC.
- The source and destination clusters should have access to the same Virtual Network (VNet). The destination cluster is a Cloud Volumes ONTAP system in Azure. The source cluster can be a Cloud Volumes ONTAP system in Azure or an ONTAP system.

Step 1: Create an additional NIC and attach to the destination VM

This section provides instructions for how to create an additional NIC and attach it to the destination VM. The destination VM is the single node or HA-pair system in Cloud Volumes ONTAP in Azure where you want to set up your additional NIC.

Steps

1. In the ONTAP CLI, stop the node.

```
dest::> halt -node <dest_node-vm>
```

2. In the Azure portal, check that the VM (node) status is stopped.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Use the Bash environment in Azure Cloud Shell to stop the node.
   a. Stop the node.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. Deallocate the node.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. Configure network security group rules to make the two subnets (source cluster subnet and destination cluster subnet) non-routable to each other.
   a. Create the new NIC on the destination VM.
   b. Look up the subnet ID for the source cluster subnet.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet -name <vnet> --query id
```

   c. Create the new NIC on the destination VM with the subnet ID for the source cluster subnet. Here you enter the name for the new NIC.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

   d. Save the privateIPAddress. This IP address, <new_added_nic_primary_addr>, is used to create an intercluster LIF in broadcast domain, intercluster LIF for the new NIC.
5. Attach the new NIC to the VM.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. Start the VM (node).

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. In the Azure portal, go to **Networking** and confirm that the new NIC, e.g. nic-new, exists and accelerated networking is enabled.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

For HA-pair deployments, repeat the steps for the partner node.

Step 2: Create a new IPspace, broadcast domain, and intercluster LIF for the new NIC

A separate IPspace for intercluster LIFs provides logical separation between networking functionality for replication between clusters.

Use the ONTAP CLI for the following steps.

Steps

1. Create the new IPspace (new_ipspace).

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. Create a broadcast domain on the new IPspace (new_ipspace) and add the nic-new port.

```
dest::> network port show
```

3. For single node systems, the newly added port is *e0b*. For HA-pair deployments with managed disks, the newly added port is *e0d*. For HA-pair deployments with page blobs, the newly added port is *e0e*. Use the node name not the VM name. Find the node name by running `node show`.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. Create an intercluster LIF on the new broadcast-domain (new_bd) and on the new NIC (nic-new).

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. Verify creation of the new intercluster LIF.

```
dest::> net int show
```

For HA-pair deployments, repeat the steps for the partner node.

Step 3: Verify cluster peering between the source and destination systems

This section provides instructions for how to verify peering between the source and destination systems.

Use the ONTAP CLI for the following steps.

Steps

1. Verify that the intercluster LIF of the destination cluster can ping the intercluster LIF of the source cluster.

Because the destination cluster executes this command, the destination IP address is the intercluster LIF IP address on the source.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. Verify that the intercluster LIF of the source cluster can ping the intercluster LIF of the destination cluster. The destination is the IP address of the new NIC created on the destination.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

For HA-pair deployments, repeat the steps for the partner node.

Step 4: Create SVM peering between the source and destination system

This section provides instructions for how to create SVM peering between the source and destination system.

Use the ONTAP CLI for the following steps.

Steps

1. Create cluster peering on the destination using the source intercluster LIF IP address as the `-peer -addrs`. For HA pairs, list the source intercluster LIF IP address for both nodes as the `-peer-addrs`.

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

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

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

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

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

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

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

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

7. Accept SVM peering.

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

8. Check that the SVM peered.

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

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

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

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

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

Use the ONTAP CLI for the following steps.

Steps

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

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

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

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

3. Initialize the SnapMirror replication relationship on the destination.

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

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

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

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

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

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

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

Google Cloud administration

Change the Google Cloud machine type for Cloud Volumes ONTAP

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

About this task

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

  ONTAP 9 Documentation: Commands for configuring automatic giveback

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

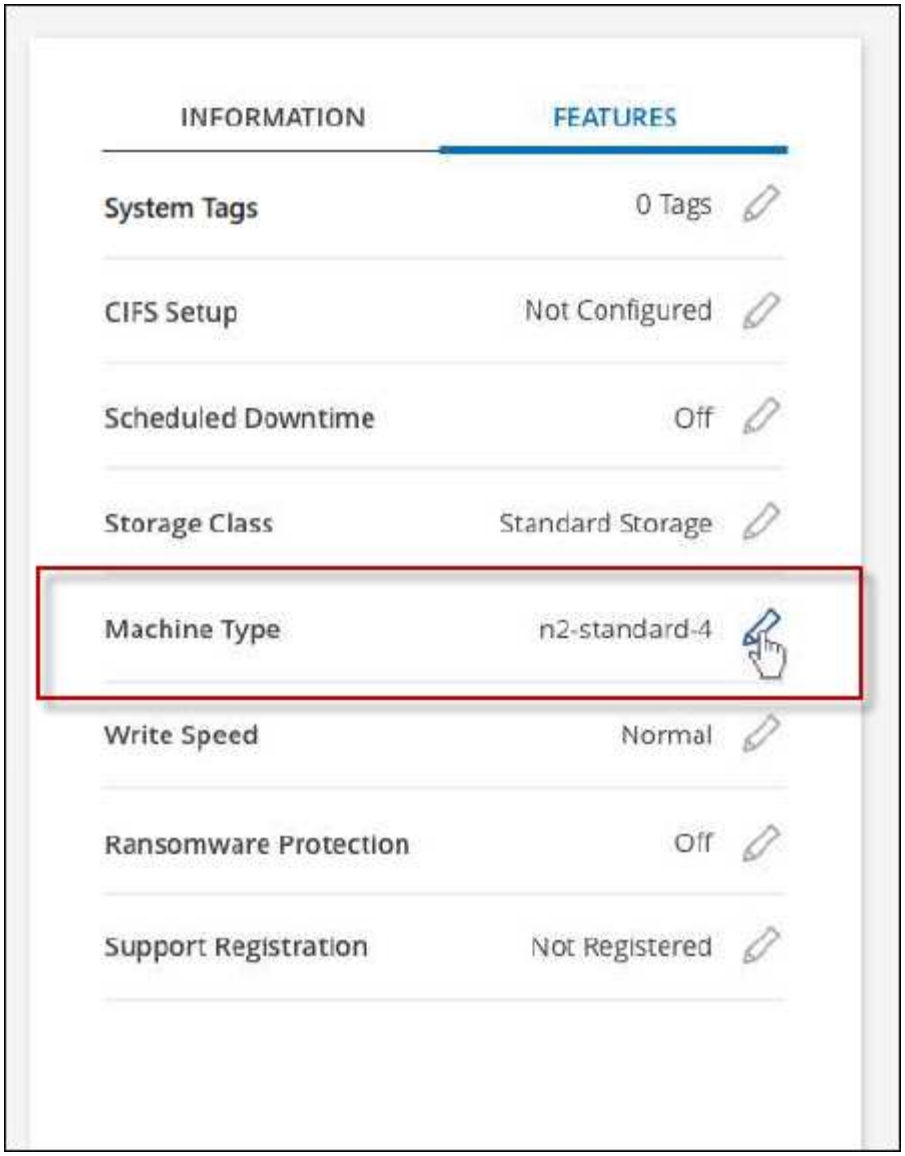
  For single node systems, I/O is interrupted.

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

The NetApp Console changes one node at a time by initiating takeover and waiting for give back. NetApp's Quality Assurance team tested both writing and reading files during this process and didn't see any issues on the client side. As connections changed, some retries were observed on the I/O level, but the application layer overcame the rewiring of NFS/CIFS connections.

Steps

1. On the **Systems** page, select the system.
2. On the Overview tab, click the Features panel and then click the pencil icon next to **Machine type**.



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

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

Result

Cloud Volumes ONTAP reboots with the new configuration.

Convert existing Cloud Volumes ONTAP deployments to Infrastructure Manager

Beginning on January 12, 2026, new Cloud Volumes ONTAP deployments in Google Cloud can use Google Cloud Infrastructure Manager. Google is about to deprecate Google Cloud Deployment Manager in favor of Infrastructure Manager. Therefore, you need to manually run a transition tool to convert your existing Cloud Volumes ONTAP deployments from Deployment Manager to Infrastructure Manager. This is a one-time process, after which your systems will automatically start using Infrastructure Manager.

About this task

The transition tool is available in the NetApp Support site, and creates the following artifacts:

- Terraform artifacts, saved in `conversion_output/deployment_name`.
- Summary of the conversion, saved in `conversion_output/batch_summary_<deployment_name>_<timestamp>.json`.
- Debug logs, saved in the `<gcp project number>-<region>-blueprint-config/<cvo name>` directory. You need these logs for troubleshooting. The `<gcp project number>-<region>-blueprint-config` bucket stores the Terraform logs.

> Cloud Volumes ONTAP systems using Infrastructure Manager store data and records in Google Cloud Storage buckets. You might incur extra costs for these buckets, but do not edit or delete the buckets or their content:
>
> - `gs://netapp-cvo-infrastructure-manager-<project id>/dm-to-im-convert`: for storing Cloud Volumes ONTAP Terraform files
> - `<gcp project number>-<region>-blueprint-config`: for storing Google Cloud Terraform artifacts

Before you begin

- Ensure that your Cloud Volumes ONTAP system is 9.16.1 or later.
- Ensure that none of the Cloud Volumes ONTAP resources or their properties have been manually edited from the Google Cloud Console.
- Ensure that the Google Cloud APIs are enabled. Refer to Enable Google Cloud APIs. Ensure that along with the other APIs, you enable the Google Cloud Quotas API.
- Verify that the NetApp Console agent's service account has all required permissions. Refer to Google Cloud permissions for the Console agent.
- The conversion tool uses the following domains. Enable them on port 443 in your network:

Domain	Port	Protocol	Direction	Purpose
cloudresourcemanager.googleapis.com	443	TCP	EGRESS	Project validation
deploymentmanager.googleapis.com	443	TCP	EGRESS	Deployment discovery
config.googleapis.com	443	TCP	EGRESS	Infrastructure Manager API
storage.googleapis.com	443	TCP	EGRESS	GCS bucket operations
iam.googleapis.com	443	TCP	EGRESS	Service account validation
compute.googleapis.com	443	TCP	EGRESS	Compute API calls used by Google Cloud and Terraform Import and Plan

Domain	Port	Protocol	Direction	Purpose
openidconnect.googleapis.com	443	TCP	EGRESS	Authentication
oauth2.googleapis.com	443	TCP	EGRESS	OAuth2 token exchange
registry.terraform.io	443	TCP	EGRESS	Terraform provider registry
releases.hashicorp.com	443	TCP	EGRESS	Terraform binary downloads
apt.releases.hashicorp.com	443	TCP	EGRESS	HashiCorp APT repository
us-central1-docker.pkg.dev	443	TCP	EGRESS	GCP Artifact Registry
metadata.google.internal	80	HTTP	Internal	VM metadata & auth tokens

Steps

Follow these steps to transition from Deployment Manager to Infrastructure Manager and run the tool for existing Cloud Volumes ONTAP deployments.

1. Create a role and attach it to a service account:
    a. Create a YAML file with the following permissions:

```
title: NetApp Dm TO IM Convert Solution
description: Permissions for the service account associated with the
VM where the tool will run.
stage: GA
includedPermissions:
- compute.addresses.get
- compute.disks.get
- compute.forwardingRules.get
- compute.healthChecks.get
- compute.instanceGroups.get
- compute.instances.get
- compute.regionBackendServices.get
- config.deployments.create
- config.deployments.get
- config.deployments.getLock
- config.deployments.lock
- config.deployments.unlock
- config.deployments.update
- config.deployments.delete
- config.deployments.updateState
- config.operations.get
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- iam.serviceAccounts.get
- storage.buckets.create
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list
```

b. Create a custom role in Google Cloud with the permissions defined in the YAML file.
`gcloud iam roles create dmtoim_convert_tool_role --project=PROJECT_ID \ --file=YAML_FILE_PATH`
For more information, refer to Creating and managing custom roles.

c. Attach the custom role to the service account that you'll use to create the VM.

d. Add the `roles/iam.serviceAccountUser` role to this service account. Refer to Service accounts overview.

2. Create a VM with the following configurations. You run the tool on this VM.
   - Machine Type: Google Compute Engine machine type e2-medium
   - OS: Ubuntu 25.10 AMD64 Minimal (image: ubuntu-minimal-2510-amd64)
   - Networking: Firewall allowing HTTP and HTTPs
   - Disk Size: 20GB

- Security: Service accounts: the service account you created
- Security: Access Scope - access set for each API:
  - Cloud Platform: Enabled
  - Compute Engine: Read only
  - Storage: Read only (default)
  - Google Cloud Logging (previously Stackdriver Logging) API: Write only (default)
  - Stackdriver Monitoring (now part of Google Cloud Operations) API: Write only (default)
  - Service Management: Read only (default)
  - Service Control: Enabled (default)
  - Google Cloud Trace (previously Stackdriver Trace): Write only (default)

3. Connect to the newly created VM using SSH: `gcloud compute ssh dmtoim-convert-executor-vm --zone <region where VM is deployed>`
4. Download the conversion tool from the NetApp Support site by using your NSS credentials: `wget <download link from NetApp Support site>`
5. Extract the downloaded TAR file: `tar -xvf <downloaded file name>`
6. Download and install these prerequisite packages:
   - Docker: 28.2.2 build 28.2.2-0ubuntu1 or later
   - Terraform: 1.14.1 or later
   - Python: 3.13.7, python3-pip, python3 venv

   ```
   sudo apt-get update
   sudo apt-get install python3-pip python3-venv -y
   wget -O - https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor
   -o /usr/share/keyrings/hashicorp-archive-keyring.gpg
   echo "deb [arch=$(dpkg --print-architecture) signed-
   by=/usr/share/keyrings/hashicorp-archive-keyring.gpg]
   https://apt.releases.hashicorp.com noble main" | sudo tee
   /etc/apt/sources.list.d/hashicorp.list
   sudo apt update && sudo apt install terraform
   sudo apt-get install -y docker.io
   sudo systemctl start docker
   ```

   Google Cloud CLI `gcloud` is preinstalled on the VM.

7. Add the current user to the Docker group, so that the tool can use Docker without `sudo` privileges.

   ```
   sudo usermod -aG docker $USER
   newgrp docker
   ```

8. Install the conversion tool:

```
cd <folder where you extracted the tool>
 ./install.sh
```

This installs the tool in an isolated environment, `dmconvert-venv`, and verifies that all required software packages are installed.

9. Enter the environment where the tool is installed: `source dmconvert-venv/bin/activate`
10. Run the conversion tool as a `non-sudo` user. Ensure that you use the same service account as the Console agent's service account, and that the service account has all the necessary permissions for Google Cloud Infrastructure Manager.

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent>
```

After you finish

The tool displays a list of all Cloud Volumes ONTAP systems and SVM details. When it finishes running, you can see the statuses of all the converted systems. Each converted system appears in the Google Console under Infrastructure Manager in a *<converted system name-imdeploy>* format, indicating that the Console now uses Infrastructure Manager APIs to manage that Cloud Volumes ONTAP system.

Post conversion, do not delete the deployment object for Deployment Manager in the Google Cloud Console. This deployment object contains metadata that Infrastructure Manager uses to manage the Cloud Volumes ONTAP systems.

If you need to roll back the conversion, you must use the same VM. If you have converted all systems and do not need to roll back to Deployment Manager, you can delete the VM.

Roll back the conversion

If you don't want to continue with the conversion, you can roll back to Deployment Manager by following these steps:

Steps

1. On the same VM that you created for running the tool, run this command:

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent> \
--rollback
```

2. Wait till the rollback is complete.

Related links

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

Administer Cloud Volumes ONTAP using System Manager

Advanced storage management capabilities in Cloud Volumes ONTAP are available through ONTAP System Manager, a management interface provided with ONTAP systems. You can access System Manager directly from the NetApp Console.

Features

You can perform various storage management functions using ONTAP System Manager in the Console. The following list includes some of those functionalities, though this list is not exhaustive:

- Advanced storage management: Manage consistency groups, shares, qtrees, quotas, and Storage VMs.
- Volume move: Move a volume to a different aggregate.
- Networking management: Manage IPspaces, network interfaces, portsets, and ethernet ports.
- Manage FlexGroup volumes: You can create and manage FlexGroup volumes only through System Manager. The Console does not support FlexGroup volume creation.
- Events and jobs: View event logs, system alerts, jobs, and audit logs.
- Advanced data protection: Protect storage VMs, LUNs, and consistency groups.
- Host management: Set up SAN initiator groups and NFS clients.
- ONTAP S3 object storage management: ONTAP S3 storage management capabilities in Cloud Volumes ONTAP are available only in System Manager, and not in the Console.

Supported configurations

- Advanced storage management through ONTAP System Manager is available in Cloud Volumes ONTAP 9.10.0 and later in standard cloud regions.
- System Manager integration is not supported in GovCloud regions or in regions that have no outbound internet access.

Limitations

A few features that appear in the System Manager interface are not supported with Cloud Volumes ONTAP:

- NetApp Cloud Tiering: Cloud Volumes ONTAP does not support Cloud Tiering. You should set up tiering of data to object storage directly from the Standard View when creating volumes.
- Tiers: Aggregate management (including local tiers and cloud tiers) is not supported from System Manager. You must manage aggregates directly from the Standard View.
- Firmware upgrades: Cloud Volumes ONTAP does not support automatic firmware updates from the **Cluster > Settings** page of the System Manager.
- Role-based access control: Role-based access control from System Manager is not supported.

- SMB Continuous Availability (CA): Cloud Volumes ONTAP does not support continuously available SMB shares for nondisruptive operations.

Configure authentication for accessing System Manager

As an administrator, you can activate authentication for users accessing ONTAP System Manager from the Console. You can determine the right level of access permissions based on the ONTAP user roles, and enable or disable authentication as needed. If you enable authentication, then users need to enter their ONTAP user credentials every time they access System Manager from the Console or when the page is reloaded, because the Console doesn't store the credentials internally. If you disable authentication, users can access System Manager using the admin credentials.

This setting is applicable for each Console agent for the ONTAP users in your organization or account, irrespective of the Cloud Volumes ONTAP system.

Required permissions

You need to be assigned the organization or account admin privileges to modify the Console agent settings for Cloud Volumes ONTAP user authentication.

Steps

1. From the left navigation pane, go to **Administration > Agents**.
2. Click the ••• icon for the required Console agent and select **Edit Console agent**.
3. Under **Force user credentials**, select the **Enable/Disable** check box. By default, authentication is disabled.

   If you set this value to **Enable**, authentication is reset, and you have to modify any existing workflows to accommodate this change.

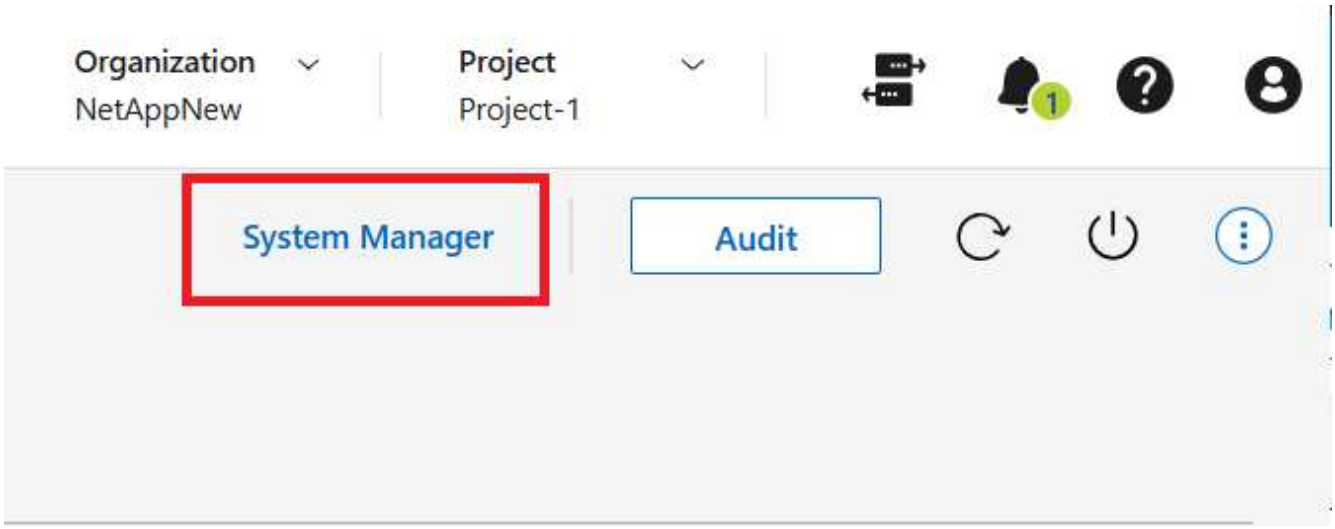
4. Click **Save**.

Get started with System Manager

You can access ONTAP System Manager from a Cloud Volumes ONTAP system.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, double click the required Cloud Volumes ONTAP system.
3. Click **System Manager**.



4. If prompted, enter your ONTAP user credentials and click **Login**.
5. If a confirmation message appears, read through it and click **Close**.

Use System Manager to manage your Cloud Volumes ONTAP system. You can click **Go back** to return to the Console.

Help with using System Manager

If you need help using System Manager with Cloud Volumes ONTAP, you can refer to the ONTAP documentation for step-by-step instructions. Here are a few ONTAP documentation links that might help:

- ONTAP roles, applications, and authentication
- Use System Manager to access a cluster.
- Volume and LUN management
- Network management
- Data protection
- Create continuously available SMB shares

Administer Cloud Volumes ONTAP from the CLI

The Cloud Volumes ONTAP CLI enables you to run all administrative commands and is a good choice for advanced tasks or if you are more comfortable using the CLI. You can connect to the CLI using Secure Shell (SSH).

Before you begin

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

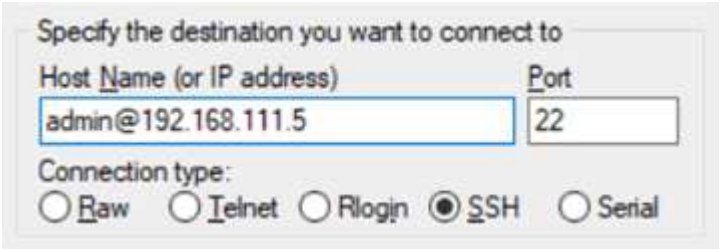
When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

Steps

1. In the NetApp Console, identify the IP address of the cluster management interface:
   a. From the left navigation menu, select **Storage > Management**.
   b. On the **Systems** page, select the Cloud Volumes ONTAP system.
   c. Copy the cluster management IP address that appears in the right pane.
2. Use SSH to connect to the cluster management interface IP address using the admin account.

   Example

   The following image shows an example using PuTTY:



3. At the login prompt, enter the password for the admin account.

   Example

```
Password: ********
COT2::>
```

Copyright information

Trademark information