Set up, upgrade and revert ONTAP
ONTAP 9
NetApp
March 08, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap/software_setup/index.html on March 08, 2024. Always check docs.netapp.com for the latest.
## Table of Contents

Set up, upgrade and revert ONTAP software and firmware .................................................. 1
  Set up ONTAP .................................................................................................................. 1
  Upgrade ONTAP ............................................................................................................ 17
  Firmware and system updates ....................................................................................... 150
  Revert ONTAP .............................................................................................................. 156
Set up, upgrade and revert ONTAP software and firmware

Set up ONTAP

Get started with ONTAP cluster set up

You can use System Manager or the ONTAP command line interface (CLI) to set up new ONTAP clusters. Before you begin, you should gather the information you’ll need to complete the cluster setup, such as your cluster management interface port and IP address.

NetApp recommends that you use System Manager to set up new clusters. System Manager provides a simple and easy workflow for cluster set up and configuration including assigning a node management IP address, initializing the cluster, creating a local tier, configuring protocols and provisioning initial storage.

It is only necessary to use the ONTAP CLI to set up your cluster if you are running ONTAP 9.7 or earlier on a MetroCluster configuration. Beginning in ONTAP 9.13.1, on the AFF A800 and FAS8700 platforms, you can also use the ONTAP CLI to create and configure new clusters in IPv6-only networking environments. If you need to use IPv6 in ONTAP 9.13.0 and earlier, or on other platforms in ONTAP 9.13.1 and later, you can use System Manager to create new clusters using IPv4 and then convert to IPv6.

What you’ll need for cluster set up

Setting up the cluster involves gathering the information needed to configure setting up each node, creating the cluster on the first node, and joining any remaining nodes to the cluster.

Get started by gathering all the relevant information in the cluster setup worksheets.

The cluster setup worksheet enables you to record the values that you need during the cluster setup process. If a default value is provided, you can use that value or else enter your own.

System defaults

The system defaults are the default values for the private cluster network. It is best to use these default values. However, if they do not meet your requirements, you can use the table to record your own values.

For clusters configured to use network switches, each cluster switch must use the 9000 MTU size.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private cluster network ports</td>
<td></td>
</tr>
<tr>
<td>Cluster network netmask</td>
<td></td>
</tr>
</tbody>
</table>
### Types of information

<table>
<thead>
<tr>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster interface IP addresses (for each cluster network port on each node)</td>
</tr>
<tr>
<td>The IP addresses for each node must be on the same subnet.</td>
</tr>
</tbody>
</table>

### Cluster information

<table>
<thead>
<tr>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster name</td>
</tr>
<tr>
<td>The name must begin with a letter, and it must be fewer than 44 characters. The name can include the following special characters:</td>
</tr>
<tr>
<td>. - _</td>
</tr>
</tbody>
</table>

### Feature license keys

You can find license keys for your initial or add-on software orders at the NetApp Support Site under **My Support > Software Licenses**.

<table>
<thead>
<tr>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature license keys</td>
</tr>
</tbody>
</table>

### Admin storage virtual machine (SVM)

<table>
<thead>
<tr>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster administrator password</td>
</tr>
<tr>
<td>The password for the admin account that the cluster requires before granting cluster administrator access to the console or through a secure protocol.</td>
</tr>
<tr>
<td>For security purposes, recording passwords in this worksheet is not recommended.</td>
</tr>
<tr>
<td>The default rules for passwords are as follows:</td>
</tr>
<tr>
<td>• A password must be at least eight characters long.</td>
</tr>
<tr>
<td>• A password must contain at least one letter and one number.</td>
</tr>
<tr>
<td>Types of information</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Cluster management interface port</td>
</tr>
<tr>
<td>Cluster management interface IP address</td>
</tr>
<tr>
<td>Cluster management interface netmask (IPv4)</td>
</tr>
<tr>
<td>Cluster management interface netmask length (IPv6)</td>
</tr>
<tr>
<td>Cluster management interface default gateway</td>
</tr>
<tr>
<td>DNS domain name</td>
</tr>
<tr>
<td>Types of information</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name server IP addresses</td>
</tr>
</tbody>
</table>

### Node information (for each node in the cluster)

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical location of the controller (optional)</td>
<td>A description of the physical location of the controller. Use a description that identifies where to find this node in the cluster (for example, “Lab 5, Row 7, Rack B”).</td>
</tr>
<tr>
<td>Node management interface port</td>
<td>The physical port that is connected to the node management network and enables the cluster administrator to manage the node.</td>
</tr>
<tr>
<td>Node management interface IP address</td>
<td>A unique IPv4 or IPv6 address for the node management interface on the management network. If you defined the node management interface port to be a data port, then this IP address should be a unique IP address on the data network. You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization. Example: 192.0.2.66</td>
</tr>
<tr>
<td>Node management interface netmask (IPv4)</td>
<td>The subnet mask that defines the range of valid IP addresses on the node management network. If you defined the node management interface port to be a data port, then the netmask should be the subnet mask for the data network. Example: 255.255.255.0</td>
</tr>
</tbody>
</table>
### Types of information

<table>
<thead>
<tr>
<th>Node management interface netmask length (IPv6)</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the node management interface uses an IPv6 address, then this value represents the prefix length that defines the range of valid IPv6 addresses on the node management network.</td>
<td>Example: 64</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Node management interface default gateway</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address for the router on the node management network.</td>
<td></td>
</tr>
</tbody>
</table>

### NTP server information

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server addresses</td>
<td>The IP addresses of the Network Time Protocol (NTP) servers at your site. These servers are used to synchronize the time across the cluster.</td>
</tr>
</tbody>
</table>

### Configure ONTAP on a new cluster with System Manager

System Manager provides a simple and easy workflow for setting up a new cluster and configuring your storage.

In some cases, such as certain MetroCluster deployments or clusters that require IPv6 network addressing, you might need to use the ONTAP CLI to set up a new cluster. Click [here](#) for more details about these requirements, as well as steps for cluster setup with the ONTAP CLI.

### Before you begin

- You should have installed, cabled and powered on your new storage system according to the installation and setup instructions for your platform model. See the [AFF and FAS documentation](#).
- Cluster network interfaces should be configured on each node of the cluster for intra-cluster communication.
- You should be aware of the following System Manager support requirements:
  - Cluster setup is supported only for single nodes and HA pairs
  - When you set up node management manually using the CLI, System Manager supports only IPv4 and does not support IPv6. However, if you launch System Manager after completing your hardware setup using DHCP with an auto assigned IP address and with Windows discovery, System Manager can configure an IPv6 management address.

In ONTAP 9.6 and earlier, System Manager does not support deployments that require IPv6 networking.
MetroCluster setup support is for MetroCluster IP configurations with two nodes at each site.

In ONTAP 9.7 and earlier, System Manager does not support new cluster setup for MetroCluster configurations.

Assign a node-management IP address

Windows System

You should connect your Windows computer to the same subnet as the controllers. This will automatically assign a node-management IP address to your system.

**Step**

1. From the Windows system, open the **Network** drive to discover the nodes.
2. Double-click the node to launch the cluster setup wizard.

**Other systems**

You should configure the node-management IP address for one of the nodes in your cluster. You can use this node-management IP address to launch the cluster setup wizard.

See [Creating the cluster on the first node](#) for information about assigning a node-management IP address.

Initialize the cluster

You initialize the cluster by setting an administrative password for the cluster and setting up the cluster management and node management networks. You can also configure services like a DNS server to resolve host names and an NTP server to synchronize time.

**Steps**

1. On a web browser, enter the node-management IP address that you have configured: "https://node-management-IP"

   System Manager automatically discovers the remaining nodes in the cluster.

2. Initialize the storage system by configuring the cluster management network and node management IP addresses for all the nodes.

Create your local tier

Create local tiers from the available disks or SSDs in your nodes. System Manager automatically calculates the best tier configuration based on your hardware.

**Steps**

1. Click **Dashboard** and then click **Prepare Storage**.

   Accept the storage recommendation for your local tier.
Configure protocols

Depending on the licenses enabled on your cluster, you can enable the desired protocols on your cluster. You then create network interfaces using which you can access the storage.

Steps

1. Click Dashboard and then click Configure Protocols.
   - Enable iSCSI or FC for SAN access.
   - Enable NFS or SMB for NAS access.
   - Enable NVMe for FC-NVMe access.

Provision Storage

After configuring protocols, you can provision storage. The options you see depend on the licenses that are installed.

Steps

1. Click Dashboard and then click Provision Storage.
   - To provision SAN access, click Add LUNs.
   - To provision NAS access, click Add Volumes.
   - To provision NVMe storage, click Add Namespaces.

Configure ONTAP on a new cluster video

Set up a cluster with the CLI
Create the cluster on the first node

You use the Cluster Setup wizard to create the cluster on the first node. The wizard helps you to configure the cluster network that connects the nodes, create the cluster admin storage virtual machine (SVM), add feature license keys, and create the node management interface for the first node.

Before you begin

- You should have installed, cabled and powered on your new storage system according to the installation and setup instructions for your platform model. See the AFF and FAS documentation.
- Cluster network interfaces should be configured on each node of the cluster for intra-cluster communication.
- If you are configuring IPv6 on your cluster, IPv6 should be configured on the Base Management Controller (BMC) so that you can access the system using SSH.

Steps

1. Power on all the nodes you are adding to the cluster. This is required to enable discovery for your cluster setup.
2. Connect to the console of the first node.
   
   The node boots, and then the Cluster Setup wizard starts on the console.

   Welcome to the cluster setup wizard....

3. Acknowledge the AutoSupport statement.

   Type yes to confirm and continue {yes}: yes

   AutoSupport is enabled by default.

4. Follow the instructions on the screen to assign an IP address to the node.

   Beginning in ONTAP 9.13.1, you can assign IPv6 addresses for management LIFs on A800 and FAS8700 platforms. For ONTAP releases earlier than 9.13.1, or for 9.13.1 and later on other platforms, you must assign IPv4 addresses for management LIFs, then convert to IPv6 after you complete cluster setup.

5. Press Enter to continue.

   Do you want to create a new cluster or join an existing cluster? {create, join}:

6. Create a new cluster: create

7. Accept the system defaults or enter your own values.

8. After setup is completed, log in to the cluster and verify that the cluster is active and the first node is
healthy by entering the ONTAP CLI command: `cluster show`

The following example shows a cluster in which the first node (cluster1-01) is healthy and eligible to participate:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01           true    true
```

You can access the Cluster Setup wizard to change any of the values you entered for the admin SVM or node SVM by using the `cluster setup` command.

**After you finish**

If needed, convert from IPv4 to IPv6.

**Join remaining nodes to the cluster**

After creating a new cluster, you use the Cluster Setup wizard to join each remaining node to the cluster one at a time. The wizard helps you to configure each node's node management interface.

When you join two nodes in a cluster, you are creating a high availability (HA) pair. If you join 4 nodes, you create two HA pairs. To learn more about HA, see [Learn about HA](#).

You can only join one node to the cluster at a time. When you start to join a node to the cluster, you must complete the join operation for that node, and the node must be part of the cluster before you can start to join the next node.

**Best Practice:** If you have a FAS2720 with 24 or fewer NL-SAS drives, you should verify that the storage configuration default is set to active/passive to optimize performance. For more information, see [Setting up an active-passive configuration on nodes using root-data partitioning](#)

1. Log in to the node you plan to join in the cluster.

   Cluster Setup wizard starts on the console.

   ```
   Welcome to the cluster setup wizard....
   ```

2. Acknowledge the AutoSupport statement.

   ![Info](https://via.placeholder.com/15/000000/000000&text=AutoSupport+is+enabled+by+default.)

   ```
   Type yes to confirm and continue {yes}: yes
   ```

3. Follow the instructions on the screen to assign an IP address to the node.
Beginning in ONTAP 9.13.1, you can assign IPv6 addresses for management LIFs on A800 and FAS8700 platforms. For ONTAP releases earlier than 9.13.1, or for 9.13.1 and later on other platforms, you must assign IPv4 addresses for management LIFs, then convert to IPv6 after you complete cluster setup.

4. Press **Enter** to continue.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

5. Join the node to the cluster: `join`

6. Follow the instructions on the screen to set up the node and join it to the cluster.

7. After setup is completed, verify that the node is healthy and eligible to participate in the cluster: `cluster show`

The following example shows a cluster after the second node (cluster1-02) has been joined to the cluster:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01           true    true
cluster1-02           true    true
```

You can access the Cluster Setup wizard to change any of the values you entered for the admin SVM or node SVM by using the `cluster setup` command.

8. Repeat this task for each remaining node.

**After you finish**

If needed, **convert from IPv4 to IPv6**.

**Convert management LIFs from IPv4 to IPv6**

Beginning in ONTAP 9.13.1, you can assign IPv6 addresses to management LIFs on A800 and FAS8700 platforms during the initial cluster setup. For ONTAP releases earlier than 9.13.1, or for 9.13.1 and later on other platforms, you must first assign IPv4 addresses to management LIFs, and then convert to IPv6 addresses after you complete cluster setup.

**Steps**

1. Enable IPv6 for the cluster:

```
network options ipv6 modify -enable true
```

2. Set privilege to advanced:
set priv advanced

3. View the list of RA prefixes learned on various interfaces:

   network ndp prefix show

4. Create an IPv6 management LIF:

   Use the format prefix::id in the address parameter to construct the IPv6 address manually.

   network interface create -vserver <svm_name> -lif <LIF> -home-node <home_node> -home-port <home_port> -address <IPv6prefix::id> -netmask -length <netmask_length> -failover-policy <policy> -service-policy <service_policy> -auto-revert true

5. Verify that the LIF was created:

   network interface show

6. Verify that the configured IP address is reachable:

   network ping6

7. Mark the IPv4 LIF as administratively down:

   network interface modify -vserver <svm_name> -lif <lif_name> -status -admin down

8. Delete the IPv4 management LIF:

   network interface delete -vserver <svm_name> -lif <lif_name>

9. Confirm that the IPv4 management LIF is deleted:

   network interface show

Check your cluster with Active IQ Config Advisor

After you have joined all the nodes to your new cluster, you should run Active IQ Config
Advisor to validate your configuration and check for common configuration errors.

Config Advisor is a web-based application that you install on your laptop, virtual machine or a server, and works across Windows, Linux, and Mac platforms.

Config Advisor runs a series of commands to validate your installation and check the overall health of the configuration, including the cluster and storage switches.

1. Download and install Active IQ Config Advisor.

   - Active IQ Config Advisor

2. Launch Active IQ, and set up a passphrase when prompted.

3. Review your settings and click Save.

4. On the Objectives page, click ONTAP Post-Deployment Validation.

5. Choose either Guided or Expert mode.

   If you choose Guided mode, connected switches are discovered automatically.

6. Enter the cluster credentials.

7. (Optional) Click Form Validate.

8. To begin collecting data, click Save & Evaluate.

9. After data collection is complete, under Job Monitor > Actions, view the data collected by clicking Data View icon, and view the results by clicking the Results icon.

10. Resolve the issues identified by Config Advisor.

**Synchronize the system time across the cluster**

Synchronizing the time ensures that every node in the cluster has the same time, and prevents CIFS and Kerberos failures.

A Network Time Protocol (NTP) server should be set up at your site. Beginning with ONTAP 9.5, you can set up your NTP server with symmetric authentication. For more information, see Managing the cluster time (cluster administrators only).

You synchronize the time across the cluster by associating the cluster with one or more NTP servers.

1. Verify that the system time and time zone is set correctly for each node.

   All nodes in the cluster should be set to the same time zone.

   a. Use the cluster date show command to display the current date, time, and time zone for each node.
b. Use the cluster date modify command to change the date or time zone for all of the nodes.

   This example changes the time zone for the cluster to be GMT:

```bash
cluster1::> cluster date modify -timezone GMT
```

2. Use the cluster time-service ntp server create command to associate the cluster with your NTP server.
   - To set up your NTP server without symmetric authentication enter the following command: `cluster time-service ntp server create -server server_name`
   - To set up your NTP server with symmetric authentication, enter the following command: `cluster time-service ntp server create -server server_ip_address -key-id key_id`

   Symmetric authentication is available Beginning with ONTAP 9.5. It is not available in ONTAP 9.4 or earlier.

   This example assumes that DNS has been configured for the cluster. If you have not configured DNS, you must specify the IP address of the NTP server:

```bash
cluster1::> cluster time-service ntp server create -server ntp1.example.com
```

3. Verify that the cluster is associated with an NTP server: `cluster time-service ntp server show`

```bash
cluster1::> cluster time-service ntp server show
Server               Version
--------------------  -----------
ntp1.example.com     auto
```

Related information

System administration
Commands for managing symmetric authentication on NTP servers

Beginning with ONTAP 9.5, Network Time Protocol (NTP) version 3 is supported. NTPv3 includes symmetric authentication using SHA-1 keys which increases network security.

<table>
<thead>
<tr>
<th>To do this…</th>
<th>Use this command…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an NTP server without symmetric authentication</td>
<td><code>cluster time-service ntp server create -server server_name</code></td>
</tr>
<tr>
<td>Configure an NTP server with symmetric authentication</td>
<td><code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code></td>
</tr>
<tr>
<td>Enable symmetric authentication for an existing NTP server</td>
<td><code>cluster time-service ntp server modify -server server_name -key-id key_id</code></td>
</tr>
<tr>
<td>An existing NTP server can be modified to enable authentication by adding the required key-id.</td>
<td><code>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</code> <strong>Note:</strong> Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server</td>
</tr>
<tr>
<td>Configure a shared NTP key</td>
<td><code>cluster time-service ntp server create -server server_name -key-id key_id</code></td>
</tr>
<tr>
<td>Configure an NTP server with an unknown key ID</td>
<td><code>cluster time-service ntp server create -server server_name -key-id key_id</code> <strong>Note:</strong> The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.</td>
</tr>
<tr>
<td>Configure a server with a key ID not configured on the NTP server.</td>
<td><code>cluster time-service ntp server create -server server_name -key-id key_id</code></td>
</tr>
<tr>
<td>Disable symmetric authentication</td>
<td><code>cluster time-service ntp server modify -server server_name -authentication disabled</code></td>
</tr>
</tbody>
</table>

**Additional system configuration tasks to complete**

After setting up a cluster, you can use either System Manager or the ONTAP command-line interface (CLI) to continue configuring the cluster.
Configure All-Flash SAN Array software

All-Flash SAN Array software configuration overview

The NetApp All-Flash SAN Arrays (ASAs) are available beginning with ONTAP 9.7. ASAs are all-flash SAN-only solutions built on proven AFF NetApp platforms.

ASA platforms use symmetric active-active for multipathing. All paths are active/optimized so in the event of a storage failover, the host does not need to wait for the ALUA transition of the failover paths to resume I/O. This reduces time to failover.

Set up an ASA

All-Flash SAN Arrays (ASAs) follow the same setup procedure as non-ASA systems.

System Manager guides you through the procedures necessary to initialize your cluster, create a local tier, configure protocols, and provision storage for your ASA.

Get started with ONTAP cluster set up.

ASA host settings and utilities

Host settings for setting up All-Flash SAN Arrays (ASAs) are the same as those for all other SAN hosts.

You can download the NetApp Host Utilities software for your specific hosts from the support site.

Ways to identify an ASA system

You can identify an ASA system using System Manager or using the ONTAP command line interface (CLI).

• From the System Manager dashboard: Click Cluster > Overview and then select the system node.
The PERSONALITY is displayed as **All-Flash SAN Array**.

- **From the CLI**: Enter the `san config show` command.

  The "All-Flash SAN Array" value returns as true for ASA systems.

**Related information**
- Technical Report 4968: NetApp All-SAN Array Data Availability and Integrity

**All-Flash SAN Array configuration limits and support**

All-Flash SAN Array (ASA) configuration limits and support varies by ONTAP version.

The most current details on supported configuration limits are available in NetApp Hardware Universe.

**SAN protocols and nodes per cluster**

ASA support for SAN protocols and nodes per cluster are as follows:

<table>
<thead>
<tr>
<th>Beginning with ONTAP...</th>
<th>Protocol support</th>
<th>Max nodes per cluster</th>
</tr>
</thead>
</table>
| 9.12.1                  | • NVMe (supported on 4-node MetroCluster IP configurations and non-MetroCluster IP configurations)  
                           • FC  
                           • iSCSI | 12 |
| 9.9.1                   | • NVMe (supported on non-MetroCluster IP configurations)  
                           • FC  
                           • iSCSI | • 12 nodes (for non-MetroCluster IP configurations)  
                           • 8 nodes (for MetroCluster IP configurations) |
| 9.7                     | • FC  
                           • iSCSI | 4 |

**Support for persistent ports**

Beginning with ONTAP 9.8, persistent ports are enabled by default on All-Flash SAN Arrays (ASAs) that are configured to use the FC protocol. Persistent ports are only available for FC and require zone membership identified by World Wide Port Name (WWPN).

Persistent ports reduce the impact of takeovers by creating a shadow LIF on the corresponding physical port of the HA partner. When a node is taken over, the shadow LIF on the partner node assumes the identity of the original LIF, including the WWPN. Before the status of path to the taken over node is changed to faulty, the shadow LIF appears as an Active/Optimized path to the host MPIO stack, and I/O is shifted. This reduces I/O disruption because the host always sees the same number of paths to the target, even during storage failover operations.
For persistent ports, the following FCP port characteristics should be identical within the HA pair:

- FCP port counts
- FCP port names
- FCP port speeds
- FCP LIF WWPN-based zoning

If any of these characteristics are not identical within the HA pair, the following EMS message is generated:

EMS : scsiblade.lif.persistent.ports.fcp.init.error

For more information on persistent ports, see NetApp Technical Report 4080: Best Practices for Modern SAN.

Upgrade ONTAP

ONTAP upgrade overview

When you upgrade your ONTAP software, you can take advantage of new and enhanced ONTAP features that can help you reduce costs, accelerate critical workloads, improve security, and expand the scope of data protection available to your organization.

A major ONTAP upgrade consists of moving from a lower to higher ONTAP numbered release. An example would be an upgrade of your cluster from ONTAP 9.8 to ONTAP 9.12.1. A minor (or patch) upgrade consists of moving from a lower ONTAP version to a higher ONTAP version within the same numbered release. An example would be an upgrade of your cluster from ONTAP 9.12.1P1 to 9.12.1P4.

To get started, you should prepare for the upgrade. If you have an active SupportEdge contract for Active IQ Digital Advisor, you should plan your upgrade with Upgrade Advisor. Upgrade Advisor provides intelligence that helps you minimize uncertainty and risk by assessing your cluster and creating an upgrade plan specific to your configuration.

After you prepare for your upgrade, it is recommended that you perform upgrades using automated non-disruptive upgrade (ANDU) from System Manager. ANDU takes advantage of ONTAP’s high-availability (HA) failover technology to ensure that clusters continue to serve data without interruption during the upgrade.

Beginning with ONTAP 9.12.1, System Manager is fully integrated with BlueXP. If BlueXP is configured on your system, you can upgrade through the BlueXP working environment.

If you want assistance upgrading your ONTAP software, NetApp Professional Services offers a Managed Upgrade Service. If you are interested in using this service, contact your NetApp sales representative or submit NetApp’s sales inquiry form. The Managed Upgrade Service as well as other types of upgrade support are available to customers with SupportEdge Expert Services at no additional cost.

When should I upgrade ONTAP?

You should upgrade your ONTAP software on a regular cadence. Upgrading ONTAP allows you to take advantage of new and enhanced features and functionality and implement current fixes for known issues.
Major ONTAP upgrades

A major ONTAP upgrade or feature release typically includes:

- New ONTAP features
- Key infrastructure changes, such as fundamental changes to NetApp WAFL operation or RAID operation
- Support for new NetApp-engineered hardware systems
- Support for replacement hardware components such as newer network interface cards or host bus adapters

New ONTAP releases are entitled to full support for 3 years. NetApp recommends that you run the newest release for 1 year after general availability (GA) and then use the remaining time within the full support window to plan for your transition to a newer ONTAP release.

ONTAP patch upgrades

Patch upgrades deliver timely fixes for critical bugs that cannot wait for the next major ONTAP feature release. Non-critical patch upgrades should be applied every 3-6 months. Critical patch upgrades should be applied as soon as possible.

Learn more about minimum recommended patch levels for ONTAP releases.

ONTAP release dates

Unresolved directive in upgrade/when-to-upgrade.adoc - include::./_include/release-dates-table.adoc[]

ONTAP support levels

Unresolved directive in upgrade/when-to-upgrade.adoc - include::./_include/support-levels-table.adoc[]

Related information

- Learn what's new in currently supported ONTAP releases.
- Learn more about minimum recommended ONTAP releases.
- Learn more about ONTAP software version support.
- Learn more about the ONTAP release model.

Execute ONTAP automated pre-upgrade checks before a planned upgrade

You don’t have to be in the process of upgrading your ONTAP software to execute the ONTAP automated upgrade pre-checks. Executing the pre-upgrade checks independently of the ONTAP automated upgrade process allows you to see which checks are performed against your cluster and gives you a list of any errors or warnings that should be corrected before you begin the actual upgrade. For example, suppose you expect to upgrade your ONTAP software during a maintenance window scheduled to occur in two weeks. While you are waiting for the scheduled date, you can run the automated upgrade pre-checks and take any necessary corrective actions in advance of your maintenance window. This will mitigate risks of unexpected configuration errors after you start your upgrade.
If you are ready to begin your ONTAP software upgrade, you do not need to perform this procedure. You should follow the automated upgrade process, which includes execution of the automated upgrade pre-checks.

For MetroCluster configurations, you should first execute these steps on Cluster A, then execute the same steps on Cluster B.

Before you begin

You should download the target ONTAP software image.

To execute the automated upgrade pre-checks for a direct multi-hop upgrade, you only need to download the software package for your target ONTAP version. You won’t need to load the intermediate ONTAP version until you begin the actual upgrade. For example, if you are executing automated pre-upgrade checks for an upgrade from 9.8 to 9.13.1, you need to download the software package for ONTAP 9.13.1. You don’t need to download the software package for ONTAP 9.12.1.
System Manager

1. Validate the ONTAP target image:

   If you are upgrading a MetroCluster configuration, you should validate Cluster A and then repeat the validation process on Cluster B.

   a. Depending on the ONTAP version that you are running, perform one of the following steps:

      | If you are running... | Do this... |
      |------------------------|------------|
      | ONTAP 9.8 or later      | Click Cluster > Overview. |
      | ONTAP 9.5, 9.6, and 9.7| Click Configuration > Cluster > Update. |
      | ONTAP 9.4 or earlier    | Click Configuration > Cluster Update. |

   b. In the right corner of the Overview pane, click ✚.
   c. Click ONTAP Update.
   d. In the Cluster Update tab, add a new image or select an available image.

      | If you want to... | Then... |
      |-------------------|--------|
      | Add a new software image from a local folder | i. Under Available Software Images, click Add from Local.  
                                                          ii. Browse to the location you saved the software image, select the image, and then click Open. |
      | Select an available image | Choose one of the listed images. |

   e. Click Validate to run the pre-upgrade validation checks.

      If any errors or warnings are found during validation, they are displayed along with a list of corrective actions. You must resolve all errors before proceeding with the upgrade. It is best
practice to also resolve warnings.

**CLI**

1. Load the target ONTAP software image into the cluster package repository:

   ```
   cluster image package get -url location
   ```

   ```
   cluster1::> cluster image package get -url
   Package download completed.
   Package processing completed.
   ```

2. Verify that the software package is available in the cluster package repository:

   ```
   cluster image package show-repository
   ```

   ```
   cluster1::> cluster image package show-repository
   Package Version  Package Build Time
   ---------------- ------------------
   9.13.1              MM/DD/YYYY 10:32:15
   ```

3. Execute the automated pre-upgrade checks:

   ```
   cluster image validate -version package_version_number -show
   -validation-details true
   ```

   If you are performing a direct multi-hop upgrade, use the target ONTAP package for verification. You don’t need to validate the intermediate upgrade image separately. For example, if you are upgrading from 9.8 to 9.13.1, you should use the 9.13.1 package for verification. You don’t need to validate the 9.12.1 package separately.

   ```
   cluster1::> cluster image validate -version 9.14.1 -show-validation
   -details true
   ```

   It can take several minutes to complete validation...
   Validation checks started successfully. Run the "cluster image show-update-progress" command to check validation status.

4. Check the validation status:
If the **Status** is "in-progress", wait and run the command again until it is completed.

```
cluster1::*> cluster image show-update-progress

Update Phase         Status                   Duration
-------------------- ----------------- ---------------
Pre-update checks    completed                00:10:00
00:01:03

Details:

Pre-update Check     Status            Error-Action
-------------------- ----------------- -------------
AMPQ Router and Broker Config Cleanup
Aggregate online status and parity check
Aggregate plex resync status check
Application Provisioning Cleanup
Autoboot Bootargs Status
Backend ...
Volume Conversion In Progress Check
Volume move progress status check
Volume online status check
iSCSI target portal groups status check
Overall Status Warning
75 entries were displayed.
```
A list of complete automated upgrade pre-checks is displayed along with any errors or warnings that should be addressed before you begin the upgrade process.

Example output
Full example output of upgrade pre-checks

cluster1::*> cluster image validate -version 9.14.1 -show-validation -details true
It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that must be performed after these automated validation checks have completed successfully. Refer to the Upgrade Advisor Plan or the "What should I verify before I upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP" documentation for the remaining manual validation checks that need to be performed before update. Upgrade ONTAP documentation available at: https://docs.netapp.com/us-en/ontap/upgrade/index.html
The list of checks are available at: https://docs.netapp.com/us-en/ontap/upgrade/task_what_to_check_before_upgrade.html
Failing to do so can result in an update failure or an I/O disruption. Please use Interoperability Matrix Tool (IMT http://mysupport.netapp.com/matrix) to verify host system supportability configuration information.

Validation checks started successfully. Run the "cluster image show-update-progress" command to check validation status.

fas2820-2n-wic-1::*> cluster image show-update-progress

<table>
<thead>
<tr>
<th>Update Phase</th>
<th>Status</th>
<th>Estimated Duration</th>
<th>Elapsed Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-update checks</td>
<td>in-progress</td>
<td>00:10:00</td>
<td>00:00:42</td>
</tr>
</tbody>
</table>

Details:

<table>
<thead>
<tr>
<th>Pre-update Check</th>
<th>Status</th>
<th>Error-Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

fas2820-2n-wic-1::*> cluster image show-update-progress

<table>
<thead>
<tr>
<th>Update Phase</th>
<th>Status</th>
<th>Estimated Duration</th>
<th>Elapsed Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-update checks</td>
<td>completed</td>
<td>00:10:00</td>
<td>00:01:03</td>
</tr>
</tbody>
</table>
### Details:

<table>
<thead>
<tr>
<th>Pre-update Check</th>
<th>Status</th>
<th>Error-Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMPQ Router and Broker Config Cleanup</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Aggregate online status and parity check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Aggregate plex resync status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Application Provisioning Cleanup</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Autoboot Bootargs Status</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Backend Configuration Status</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Boot Menu Status</td>
<td>Warning</td>
<td>Warning: bootarg.init.bootmenu is enabled on nodes: fas2820-wic-1a, fas2820-wic-1b. The boot process of the nodes will be delayed. Action: Set the bootarg.init.bootmenu bootarg to false before proceeding with the upgrade.</td>
</tr>
<tr>
<td>Broadcast Domain availability and uniqueness for HA pair status</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>CIFS compatibility status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>CLAM quorum online status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>CPU Utilization Status</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Capacity licenses install status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Check For SP/BMC Connectivity To Nodes</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Check</td>
<td>Result</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>Check LDAP fastbind</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>users using unsecure connection.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check for unsecure kex algorithm configurations.</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Check for unsecure mac configurations.</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Cloud keymanager connectivity check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Cluster health and eligibility status</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Cluster quorum status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Cluster/management switch check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Compatible New Image Check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Current system version check if it is susceptible to possible outage during NDU</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Data ONTAP Version and Previous Upgrade Status</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Data aggregates HA policy check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Disk status check for failed, broken or non-compatibility</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Duplicate Initiator Check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Encryption key migration status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>External key-manager with legacy KMIP client check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>External keymanager key server status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Fabricpool Object Store Availability High Availability</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration</td>
<td>Status</td>
<td>Details</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Infinite Volume</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Availability check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LIF failover</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Capability status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LIF health check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>LIF load balancing</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Status check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LIFs is on home</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Node status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logically over</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Allocated DP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volumes check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MetroCluster</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status check for</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compatibility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum number of</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Aggregate disks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAE Aggregate and</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>NVE Volume</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption Check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDMP sessions check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>NFS mounts status</td>
<td>Warning</td>
<td>N/A</td>
</tr>
<tr>
<td>Check</td>
<td></td>
<td>Warning: This cluster is serving clients. If NFS soft mounts are used, there is a possibility of frequent NFS timeouts and race conditions that can lead to data corruption during the upgrade. Action: Use NFS hard mounts, if possible. To list Vservers running NFS, run the following command: vserver nfs show</td>
</tr>
<tr>
<td>Name Service</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration DNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name Service</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration LDAP Check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----</td>
<td>-----</td>
</tr>
<tr>
<td>Node to SP/BMC connectivity check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>OKM/KMIP enabled systems - Missing keys check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>ONTAP API to REST transition warning</td>
<td>Warning</td>
<td>Warning: NetApp ONTAP API has been used on this cluster for ONTAP storage management within the last 30 days. NetApp ONTAP API is approaching end of availability. Action: Transition your automation tools from ONTAP API to ONTAP REST API. For more details, refer to CPC-00410 - End of availability: ONTAPI</td>
</tr>
<tr>
<td>ONTAP Image Capability Status</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>OpenSSL 3.0.x upgrade validation check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Openssh 7.2 upgrade validation check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Platform Health Monitor check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Pre-Update Configuration Verification</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>RDB Replica Health Check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Replicated database schema consistency check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Running Jobs Status</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>SAN LIF association status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Feature</td>
<td>Status</td>
<td>Details</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>SAN compatibility for manual configurability check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>SAN kernel agent status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Secure Purge operation Check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Shelves and Sensors check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>SnapLock Version Check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>SnapMirror Synchronous relationship status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>SnapMirror compatibility status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Supported platform check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Target ONTAP release support for FiberBridge 6500N check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Upgrade Version Compatibility Status</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Verify all bgp peer-groups are in the up state</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Verify if a cluster management LIF exists</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Verify that e0M is home to no LIFs with high speed services.</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Volume Conversion In Progress Check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Volume move progress status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>Volume online status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>iSCSI target portal groups status check</td>
<td>OK</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Prepare for an ONTAP upgrade

Properly preparing for an ONTAP software upgrade helps you identify and mitigate potential upgrade risks or blockers before you begin the upgrade process. During upgrade preparation, you can also identify any special considerations you might need to account for before you upgrade. For example, if SSL FIPs mode is enabled on your cluster and the administrator accounts use SSH public keys for authentication, you need to verify that the host key algorithm is supported in your target ONTAP release.

You should do the following to prepare for an upgrade:

1. **Create an upgrade plan.**
   - If you have an active SupportEdge contract for Active IQ Digital Advisor, plan your upgrade with Upgrade Advisor. If you do not have access to Active IQ Digital Advisor, create your own upgrade plan.

2. **Choose your target ONTAP release.**

3. **Review the ONTAP release notes** for the target release.
   - The “Upgrade cautions” section describes potential issues that you should be aware of before upgrading to the new release. The “What’s new” and “Known problems and limitations” sections describe new system behavior after upgrading to the new release.

4. **Confirm ONTAP support for your hardware configuration.**
   - Your hardware platform, cluster management switches and MetroCluster IP switches must support the target release. If your cluster is configured for SAN, the SAN configuration must be fully supported.

5. **Use Active IQ Config Advisor to verify that you have no common configuration errors.**

6. **Review the supported ONTAP upgrade paths** to determine if you can perform a direct upgrade or if you need to complete the upgrade in stages.

7. **Verify your LIF failover configuration.**
   - Before you perform an upgrade, you need to verify that the cluster’s failover policies and failover groups are configured correctly.

8. **Verify your SVM routing configuration.**

9. **Verify special considerations** for your cluster.
   - If certain configurations exist on your cluster, there are specific actions you need to take before you begin an ONTAP software upgrade.

10. **Reboot the SP or BMC.**
Create an ONTAP upgrade plan

It is a best practice to create an upgrade plan. If you have an active SupportEdge Services contract for Active IQ Digital Advisor, you can use Upgrade Advisor to generate an upgrade plan. Otherwise, you should create your own plan.

Plan your upgrade with Upgrade Advisor

The Upgrade Advisor service in Active IQ Digital Advisor provides intelligence that helps you plan your upgrade and minimizes uncertainty and risk.

Active IQ identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP. The Upgrade Advisor service helps you plan for a successful upgrade and provides a report of issues you might need to be aware of in the ONTAP version you’re upgrading to.

Steps

1. Launch Active IQ
2. In Active IQ view any risks associated with your cluster and manually take corrective actions.
   
   Risks included in the SW Config Change, HW Config Change, and HW Replacement categories need to be resolved prior to performing an ONTAP upgrade.
3. Review the recommended upgrade path and generate your upgrade plan.

How long will an ONTAP upgrade take?

You should plan for at least 30 minutes to complete preparatory steps for an ONTAP upgrade, 60 minutes to upgrade each HA pair, and at least 30 minutes to complete post-upgrade steps.

   If you are using NetApp Encryption with an external key management server and the Key Management Interoperability Protocol (KMIP), you should expect the upgrade for each HA pair to be longer than one hour.

These upgrade duration guidelines are based on typical configurations and workloads. You can use these guidelines to estimate the time it will take to perform a nondisruptive upgrade in your environment. The actual duration of your upgrade process will depend on your individual environment and the number of nodes.

Choose your target ONTAP release for an upgrade

When you use Upgrade Advisor to generate an upgrade plan for your cluster, the plan includes a recommended target ONTAP release for upgrade. The recommendation given by Upgrade Advisor is based on your current configuration and your current ONTAP version.

If you do not use Upgrade Advisor to plan your upgrade, you should choose your target ONTAP release for the upgrade based on NetApp recommendations or your need to be at the minimum release to meet your for performance needs.

• Upgrade to the latest available release (recommended)

   NetApp recommends that you upgrade your ONTAP software to the latest patch version of the latest numbered ONTAP release. If this is not possible because the latest numbered release is not supported by
the storage systems in your cluster, you should upgrade to the latest numbered release that is supported.

- Minimum recommended release

If you want to restrict your upgrade to the minimum recommended release for your cluster, see Minimum recommended ONTAP releases to determine the ONTAP version you should upgrade to.

**Confirm ONTAP support for your hardware configuration**

Before you upgrade ONTAP, you should confirm that your hardware configuration can support the target ONTAP release.

**All configurations**

Use NetApp Hardware Universe to confirm that your hardware platform and cluster and management switches are supported in the target ONTAP release. Cluster and management switches include the cluster network switches (NX-OS), management network switches (IOS), and reference configuration file (RCF). If your cluster and management switches are supported but are not running the minimum software versions required for the target ONTAP release, upgrade your switches to supported software versions.

- NetApp Downloads: Broadcom Cluster Switches
- NetApp Downloads: Cisco Ethernet Switches
- NetApp Downloads: NetApp Cluster Switches

If you need to upgrade your switches, NetApp recommends that you complete the ONTAP software upgrade first, then perform the software upgrade for your switches.

**MetroCluster configurations**

Before you upgrade ONTAP, if you have a MetroCluster configuration, use the NetApp Interoperability Matrix Tool to confirm that your MetroCluster IP switches are supported in the target ONTAP release.

**SAN configurations**

Before you upgrade ONTAP, if your cluster is configured for SAN, use the NetApp Interoperability Matrix Tool to confirm that the SAN configuration is fully supported.

All SAN components—including the target ONTAP software version, host OS and patches, required Host Utilities software, multipathing software, and adapter drivers and firmware—should be supported.

**Identify configuration errors with Active IQ Config Advisor**

Before you upgrade ONTAP, you can use the Active IQ Config Advisor tool to check for common configuration errors.

Active IQ Config Advisor is a configuration validation tool for NetApp systems. It can be deployed at both secure sites and nonsecure sites for data collection and system analysis.

- Support for Active IQ Config Advisor is limited and is available only online.

**Steps**
1. Log in to the NetApp Support Site, and then click TOOLS > Tools.

2. Under Active IQ Config Advisor, click Download App.

3. Download, install, and run Active IQ Config Advisor.

4. After running Active IQ Config Advisor, review the tool's output, and follow the recommendations that are provided to address any issues discovered by the tool.

Supported ONTAP upgrade paths

The version of ONTAP that you can upgrade to depends on your hardware platform and the version of ONTAP currently running on your cluster’s nodes.

To verify that your hardware platform is supported for the target upgrade release, see NetApp Hardware Universe. Use the NetApp Interoperability Matrix Tool to confirm support for your configuration.

To determine your current ONTAP version:

- In System Manager, click Cluster > Overview.
- From the command line interface (CLI), use the cluster image show command. You can also use the system node image show command at the advanced privilege level to display details.

Types of upgrade paths

Automated nondisruptive upgrades (ANDU) are recommended whenever possible. Depending on your current and target releases, your upgrade path will be direct, direct multi-hop, or multi-stage.

- Direct
  You can always upgrade directly to the next adjacent ONTAP release family using a single software image. For most releases, you can also install a software image that allows you to upgrade directly to releases that are two releases higher than the running release.

  For example, you can use the direct update path from 9.8 to 9.9.1, or from 9.8 to 9.10.1.

  **Note:** Beginning with ONTAP 9.11.1, software images support upgrading directly to releases that are three or more releases higher than the running release. For example, you can use the direct upgrade path from 9.8 to 9.12.1.

  All direct upgrade paths are supported for mixed version clusters.

- Direct multi-hop
  For some automated nondisruptive upgrades (ANDU) to non-adjacent releases, you need to install the software image for an intermediate release as well the target release. The automated upgrade process uses the intermediate image in the background to complete the update to the target release.

  For example, if the cluster is running 9.3 and you want to upgrade to 9.7, you would load the ONTAP install packages for both 9.5 and 9.7, then initiate ANDU to 9.7. ONTAP automatically upgrades the cluster first to 9.5 and then to 9.7. You should expect multiple takeover/giveback operations and related reboots during the process.

- Multi-stage
  If a direct or direct multi-hop path is not available for your non-adjacent target release, you must first upgrade to a supported intermediate release, and then upgrade to the target release.
For example, if you are currently running 9.6 and you want to upgrade to 9.11.1, you must complete a multi-stage upgrade: first from 9.6 to 9.8, and then from 9.8 to 9.11.1. Upgrades from earlier releases might require three or more stages, with several intermediate upgrades.

**Note:** Before beginning multi-stage upgrades, be sure your target release is supported on your hardware platform.

Before you begin any major upgrade, it is a best practice to upgrade first to the latest patch release of the ONTAP version running on your cluster. This will ensure that any issues in your current version of ONTAP are resolved before upgrading.

For example, if your system is running ONTAP 9.3P9 and you are planning to upgrade to 9.11.1, you should first upgrade to the latest 9.3 patch release, then follow the upgrade path from 9.3 to 9.11.1.

Learn about Minimum Recommended ONTAP releases on the NetApp Support Site.

**Supported upgrade paths**

The following upgrade paths are supported for automated and manual upgrades of your ONTAP software. These upgrade paths apply to on-premises ONTAP and ONTAP Select. There are different supported upgrade paths for Cloud Volumes ONTAP.

**For mixed version ONTAP clusters:** All *direct* and *direct multi-hop* upgrade paths include ONTAP versions that are compatible for mixed version clusters. ONTAP versions included in *multi-stage* upgrades are not compatible for mixed version clusters. For example, an upgrade from 9.8 to 9.12.1 is a *direct* upgrade. A cluster with nodes running 9.8 and 9.12.1 is a supported mixed version cluster. An upgrade from 9.8 to 9.13.1 is a *multi-stage* upgrade. A cluster with nodes running 9.8 and 9.13.1 is not a supported mixed version cluster.

**From ONTAP 9.10.1 and later**

Automated and manual upgrades from ONTAP 9.10.1 and later follow the same upgrade paths.

<table>
<thead>
<tr>
<th>If your current ONTAP release is...</th>
<th>And your target ONTAP release is...</th>
<th>Your automated or manual upgrade path is...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9.13.1</td>
<td>direct</td>
</tr>
<tr>
<td>9.11.1</td>
<td>9.14.1</td>
<td>direct</td>
</tr>
<tr>
<td></td>
<td>9.13.1</td>
<td>direct</td>
</tr>
<tr>
<td></td>
<td>9.12.1</td>
<td>direct</td>
</tr>
<tr>
<td>9.10.1</td>
<td>9.14.1</td>
<td>direct</td>
</tr>
<tr>
<td></td>
<td>9.13.1</td>
<td>direct</td>
</tr>
<tr>
<td></td>
<td>9.12.1</td>
<td>direct</td>
</tr>
<tr>
<td></td>
<td>9.11.1</td>
<td>direct</td>
</tr>
</tbody>
</table>
### From ONTAP 9.9.1

Automated and manual upgrades from ONTAP 9.9.1 follow the same upgrade paths.

<table>
<thead>
<tr>
<th>If your current ONTAP release is...</th>
<th>And your target ONTAP release is...</th>
<th>Your automated or manual upgrade path is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9.1</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.9.1→9.13.1</td>
</tr>
<tr>
<td></td>
<td>9.13.1</td>
<td>direct</td>
</tr>
<tr>
<td></td>
<td>9.12.1</td>
<td>direct</td>
</tr>
<tr>
<td></td>
<td>9.11.1</td>
<td>direct</td>
</tr>
<tr>
<td></td>
<td>9.10.1</td>
<td>direct</td>
</tr>
</tbody>
</table>

### From ONTAP 9.8

Automated and manual upgrades from ONTAP 9.8 follow the same upgrade paths.

If you are upgrading a MetroCluster IP configuration from 9.8 to 9.10.1 or later on any of the following platforms, you must upgrade to 9.9.1 before you upgrade to 9.10.1 or later.

- FAS2750
- FAS500f
- AFF A220
- AFF A250

Clusters in MetroCluster IP configurations on these platforms cannot be upgraded directly 9.8 to 9.10.1 or later. The listed direct upgrade paths can be used for all other platforms.

<table>
<thead>
<tr>
<th>If your current ONTAP release is...</th>
<th>And your target ONTAP release is...</th>
<th>Your automated or and manual upgrade path is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.8 → 9.12.1</td>
</tr>
<tr>
<td></td>
<td>9.13.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.8 → 9.12.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.12.1 → 9.13.1</td>
</tr>
<tr>
<td></td>
<td>9.12.1</td>
<td>direct</td>
</tr>
<tr>
<td></td>
<td>9.11.1</td>
<td>direct</td>
</tr>
<tr>
<td></td>
<td>9.10.1</td>
<td>direct</td>
</tr>
<tr>
<td></td>
<td>9.9.1</td>
<td>direct</td>
</tr>
</tbody>
</table>
From ONTAP 9.7

The upgrade paths from ONTAP 9.7 might vary based upon whether you are performing an automated or a manual upgrade.
## Automated paths

<table>
<thead>
<tr>
<th>If your current ONTAP release is...</th>
<th>And your target ONTAP release is...</th>
<th>Your automated upgrade path is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.7</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.7 → 9.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.8 → 9.12.1</td>
</tr>
<tr>
<td>9.13.1</td>
<td></td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.7 → 9.9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.9.1 → 9.13.1</td>
</tr>
<tr>
<td>9.12.1</td>
<td></td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.7 → 9.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.8 → 9.12.1</td>
</tr>
<tr>
<td>9.11.1</td>
<td></td>
<td>direct multi-hop (requires images for 9.8 and 9.11.1)</td>
</tr>
<tr>
<td>9.10.1</td>
<td></td>
<td>direct multi-hop (requires images for 9.8 and 9.10.1P1 or later P release)</td>
</tr>
<tr>
<td>9.9.1</td>
<td></td>
<td>direct</td>
</tr>
<tr>
<td>9.8</td>
<td></td>
<td>direct</td>
</tr>
</tbody>
</table>

## Manual paths

<table>
<thead>
<tr>
<th>If your current ONTAP release is...</th>
<th>And your target ONTAP release is...</th>
<th>Your manual upgrade path is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.7</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.7 → 9.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.8 → 9.12.1</td>
</tr>
<tr>
<td>9.13.1</td>
<td></td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.7 → 9.9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-9.9.1 → 9.13.1</td>
</tr>
<tr>
<td>9.12.1</td>
<td></td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.8 → 9.12.1</td>
</tr>
<tr>
<td>9.11.1</td>
<td></td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.8 → 9.11.1</td>
</tr>
<tr>
<td>9.10.1</td>
<td></td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.8 → 9.10.1</td>
</tr>
<tr>
<td>9.9.1</td>
<td></td>
<td>direct</td>
</tr>
<tr>
<td>9.8</td>
<td></td>
<td>direct</td>
</tr>
</tbody>
</table>
From ONTAP 9.6

The upgrade paths from ONTAP 9.6 might vary based upon whether you are performing an automated or a manual upgrade.
<table>
<thead>
<tr>
<th>If your current ONTAP release is…</th>
<th>And your target ONTAP release is…</th>
<th>Your automated upgrade path is…</th>
</tr>
</thead>
</table>
| 9.6                             | 9.14.1                          | multi-stage  
-9.6 → 9.8  
-9.8 → 9.12.1  
| 9.13.1                          | multi-stage  
-9.6 → 9.8  
-9.8 → 9.12.1  
-9.12.1 → 9.13.1 |
| 9.12.1                          | multi-stage  
- 9.6 → 9.8  
-9.8 → 9.12.1 |
| 9.11.1                          | multi-stage  
- 9.6 → 9.8  
- 9.8 → 9.11.1 |
| 9.10.1                          | direct multi-hop  
(requires images for 9.8 and 9.10.1P1 or later P release) |
| 9.9.1                           | multi-stage  
- 9.6 → 9.8  
- 9.8 → 9.9.1 |
<p>| 9.8                             | direct                         |
| 9.7                             | direct                         |</p>
<table>
<thead>
<tr>
<th>If your current ONTAP release is...</th>
<th>And your target ONTAP release is...</th>
<th>Your manual upgrade path is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.6</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.6 → 9.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.8 → 9.12.1</td>
</tr>
<tr>
<td>9.13.1</td>
<td>multi-stage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.6 → 9.8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.8 → 9.12.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.12.1 → 9.13.1</td>
<td></td>
</tr>
<tr>
<td>9.12.1</td>
<td>multi-stage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.6 → 9.8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.8 → 9.12.1</td>
<td></td>
</tr>
<tr>
<td>9.11.1</td>
<td>multi-stage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.6 → 9.8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.8 → 9.11.1</td>
<td></td>
</tr>
<tr>
<td>9.10.1</td>
<td>multi-stage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.6 → 9.8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.8 → 9.10.1</td>
<td></td>
</tr>
<tr>
<td>9.9.1</td>
<td>multi-stage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.6 → 9.8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.8 → 9.9.1</td>
<td></td>
</tr>
<tr>
<td>9.8</td>
<td>direct</td>
<td></td>
</tr>
<tr>
<td>9.7</td>
<td>direct</td>
<td></td>
</tr>
</tbody>
</table>

From ONTAP 9.5

The upgrade paths from ONTAP 9.5 might vary based upon whether you are performing an automated or a manual upgrade.
### Automated paths

<table>
<thead>
<tr>
<th>If your current ONTAP release is...</th>
<th>And your target ONTAP release is...</th>
<th>Your automated upgrade path is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.13.1</td>
</tr>
<tr>
<td>9.13.1</td>
<td></td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.13.1</td>
</tr>
<tr>
<td>9.12.1</td>
<td></td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.12.1</td>
</tr>
<tr>
<td>9.11.1</td>
<td></td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.11.1</td>
</tr>
<tr>
<td>9.10.1</td>
<td></td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.10.1</td>
</tr>
<tr>
<td>9.9.1</td>
<td></td>
<td>direct multi-hop (requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td>9.8</td>
<td></td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.8</td>
</tr>
<tr>
<td>9.7</td>
<td></td>
<td>direct</td>
</tr>
<tr>
<td>9.6</td>
<td></td>
<td>direct</td>
</tr>
</tbody>
</table>

### Manual upgrade paths
<table>
<thead>
<tr>
<th>If your current ONTAP release is...</th>
<th>And your target ONTAP release is...</th>
<th>Your manual upgrade path is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.12.1</td>
</tr>
<tr>
<td>9.13.1</td>
<td>multi-stage</td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.12.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.12.1 → 9.13.1</td>
</tr>
<tr>
<td>9.12.1</td>
<td>multi-stage</td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.12.1</td>
</tr>
<tr>
<td>9.11.1</td>
<td>multi-stage</td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.11.1</td>
</tr>
<tr>
<td>9.10.1</td>
<td>multi-stage</td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.10.1</td>
</tr>
<tr>
<td>9.9.1</td>
<td>multi-stage</td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.9.1</td>
</tr>
<tr>
<td>9.8</td>
<td>multi-stage</td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.8</td>
</tr>
<tr>
<td>9.7</td>
<td>direct</td>
<td></td>
</tr>
<tr>
<td>9.6</td>
<td>direct</td>
<td></td>
</tr>
</tbody>
</table>

**From ONTAP 9.4-9.0**

The upgrade paths from ONTAP 9.4, 9.3, 9.2, 9.1 and 9.0 might vary based upon whether you are performing an automated upgrade or a manual upgrade.
## Automated upgrade

<table>
<thead>
<tr>
<th>If your current ONTAP release is...</th>
<th>And your target ONTAP release is...</th>
<th>Your automated upgrade path is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.4</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.4 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.13.1</td>
</tr>
<tr>
<td>9.13.1</td>
<td>multi-stage</td>
<td>- 9.4 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.13.1</td>
</tr>
<tr>
<td>9.12.1</td>
<td>multi-stage</td>
<td>- 9.4 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.12.1</td>
</tr>
<tr>
<td>9.11.1</td>
<td>multi-stage</td>
<td>- 9.4 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.11.1</td>
</tr>
<tr>
<td>9.10.1</td>
<td>multi-stage</td>
<td>- 9.4 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.10.1</td>
</tr>
<tr>
<td>9.9.1</td>
<td>multi-stage</td>
<td>- 9.4 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)</td>
</tr>
<tr>
<td>9.8</td>
<td>multi-stage</td>
<td>- 9.4 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.8 (direct multi-hop, requires images for 9.7 and 9.8)</td>
</tr>
<tr>
<td>9.7</td>
<td>multi-stage</td>
<td>- 9.4 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td>9.6</td>
<td>multi-stage</td>
<td>- 9.4 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.6</td>
</tr>
<tr>
<td>9.5</td>
<td>direct</td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your automated upgrade path is...</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>9.3</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.13.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.13.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.12.1</td>
</tr>
<tr>
<td>9.11.1</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.9.1 → 9.11.1</td>
</tr>
<tr>
<td>9.10.1</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.10.1 (direct multi-hop, requires images for 9.8 and 9.10.1)</td>
</tr>
<tr>
<td>9.9.1</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.9.1</td>
</tr>
<tr>
<td>9.8</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.8</td>
</tr>
<tr>
<td>9.7</td>
<td>9.14.1</td>
<td>direct multi-hop (requires images for 9.5 and 9.7)</td>
</tr>
<tr>
<td>9.6</td>
<td>9.14.1</td>
<td>multi-stage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.6</td>
</tr>
<tr>
<td>9.5</td>
<td>9.14.1</td>
<td>direct</td>
</tr>
<tr>
<td>9.4</td>
<td>9.14.1</td>
<td>not available</td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your automated upgrade path is...</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>9.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your automated upgrade path is...</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>9.7</td>
<td>multi-stage</td>
<td>- 9.2 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.6</td>
<td>multi-stage</td>
<td>- 9.2 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.6</td>
</tr>
<tr>
<td>9.5</td>
<td>multi-stage</td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.6</td>
</tr>
<tr>
<td>9.4</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>9.3</td>
<td>direct</td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your automated upgrade path is...</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>9.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your automated upgrade path is...</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>9.7</td>
<td>multi-stage</td>
<td>9.7 → 9.8 (direct multi-hop, requires images for 9.5 and 9.7)</td>
</tr>
<tr>
<td></td>
<td>- 9.1 → 9.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.3 → 9.6 (direct multi-hop, requires images for 9.5 and 9.6)</td>
<td></td>
</tr>
<tr>
<td>9.6</td>
<td>multi-stage</td>
<td>9.6 → 9.3 (direct multi-hop, requires images for 9.5 and 9.6)</td>
</tr>
<tr>
<td></td>
<td>- 9.1 → 9.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.3 → 9.6 (direct multi-hop, requires images for 9.5 and 9.6)</td>
<td></td>
</tr>
<tr>
<td>9.5</td>
<td>multi-stage</td>
<td>9.5 → 9.3 (direct multi-hop, requires images for 9.5 and 9.6)</td>
</tr>
<tr>
<td></td>
<td>- 9.1 → 9.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 9.3 → 9.5</td>
<td></td>
</tr>
<tr>
<td>9.4</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>9.3</td>
<td>direct</td>
<td></td>
</tr>
<tr>
<td>9.2</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your automated upgrade path is...</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>9.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your automated upgrade path is...</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>9.8</td>
<td>multi-stage</td>
<td>- 9.0 → 9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.8</td>
</tr>
<tr>
<td>9.7</td>
<td>multi-stage</td>
<td>- 9.0 → 9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.8</td>
</tr>
<tr>
<td>9.6</td>
<td>multi-stage</td>
<td>- 9.0 → 9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.6</td>
</tr>
<tr>
<td>9.5</td>
<td>multi-stage</td>
<td>- 9.0 → 9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td>9.4</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>9.3</td>
<td>multi-stage</td>
<td>- 9.0 → 9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td>9.2</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>9.1</td>
<td>direct</td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your ANDU upgrade path is...</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------</td>
<td>-------------------------------</td>
</tr>
</tbody>
</table>
| 9.4                              | 9.14.1                             | multi-stage  
- 9.4 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1  
| 9.13.1                           | multi-stage  
- 9.4 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1  
- 9.12.1 → 9.13.1 |
| 9.12.1                           | multi-stage  
- 9.4 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1  
- 9.9.1 → 9.12.1 |
| 9.11.1                           | multi-stage  
- 9.4 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1  
- 9.9.1 → 9.11.1 |
| 9.10.1                           | multi-stage  
- 9.4 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1  
- 9.9.1 → 9.10.1 |
| 9.9.1                            | multi-stage  
- 9.4 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1 |
| 9.8                              | multi-stage  
- 9.4 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.8 |
| 9.7                              | multi-stage  
- 9.4 → 9.5  
- 9.5 → 9.7 |
| 9.6                              | multi-stage  
- 9.4 → 9.5  
- 9.5 → 9.6 |
<p>| 9.5                              | direct |</p>
<table>
<thead>
<tr>
<th>If your current ONTAP release is...</th>
<th>And your target ONTAP release is...</th>
<th>Your ANDU upgrade path is...</th>
</tr>
</thead>
</table>
| 9.3                                | 9.14.1                               | multi-stage  
- 9.3 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1  
- 9.9.1 → 9.12.1  
| 9.13.1                             | multi-stage  
- 9.3 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1  
- 9.9.1 → 9.12.1  
- 9.12.1 → 9.13.1 |
| 9.12.1                             | multi-stage  
- 9.3 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1  
- 9.9.1 → 9.12.1 |
| 9.11.1                             | multi-stage  
- 9.3 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1  
- 9.9.1 → 9.11.1 |
| 9.10.1                             | multi-stage  
- 9.3 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1  
- 9.9.1 → 9.10.1 |
| 9.9.1                              | multi-stage  
- 9.3 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.9.1 |
| 9.8                                | multi-stage  
- 9.3 → 9.5  
- 9.5 → 9.7  
- 9.7 → 9.8 |
| 9.7                                | multi-stage  
- 9.3 → 9.5  
- 9.5 → 9.7 |
| 9.6                                | multi-stage  
- 9.3 → 9.5  
- 9.5 → 9.6 |
<p>| 9.5                                | direct |
| 9.4                                | not available |</p>
<table>
<thead>
<tr>
<th>If your current ONTAP release is...</th>
<th>And your target ONTAP release is...</th>
<th>Your ANDU upgrade path is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your ANDU upgrade path is...</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>9.7</td>
<td>multi-stage</td>
<td>- 9.2 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td>9.6</td>
<td>multi-stage</td>
<td>- 9.2 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.6</td>
</tr>
<tr>
<td>9.5</td>
<td>multi-stage</td>
<td>- 9.2 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td>9.4</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>9.3</td>
<td>direct</td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your ANDU upgrade path is...</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>9.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your ANDU upgrade path is...</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>9.7</td>
<td>multi-stage</td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td>9.6</td>
<td>multi-stage</td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.6</td>
</tr>
<tr>
<td>9.5</td>
<td>multi-stage</td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td>9.4</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>9.3</td>
<td>direct</td>
<td></td>
</tr>
<tr>
<td>9.2</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your ANDU upgrade path is...</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>9.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If your current ONTAP release is...</td>
<td>And your target ONTAP release is...</td>
<td>Your AUD upgrade path is...</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>9.8</td>
<td>multi-stage</td>
<td>- 9.0 → 9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.7 → 9.8</td>
</tr>
<tr>
<td>9.7</td>
<td>multi-stage</td>
<td>- 9.0 → 9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.7</td>
</tr>
<tr>
<td>9.6</td>
<td>multi-stage</td>
<td>- 9.0 → 9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.5 → 9.6</td>
</tr>
<tr>
<td>9.5</td>
<td>multi-stage</td>
<td>- 9.0 → 9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.3 → 9.5</td>
</tr>
<tr>
<td>9.4</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>9.3</td>
<td>multi-stage</td>
<td>- 9.0 → 9.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 9.1 → 9.3</td>
</tr>
<tr>
<td>9.2</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>9.1</td>
<td>direct</td>
<td></td>
</tr>
</tbody>
</table>

**Data ONTAP 8**

Be sure to verify that your platform can run the target ONTAP release by using the NetApp Hardware Universe.

**Note:** The Data ONTAP 8.3 Upgrade Guide erroneously states that in a four-node cluster, you should plan to upgrade the node that holds epsilon last. This is no longer a requirement for upgrades beginning with Data ONTAP 8.2.3. For more information, see NetApp Bugs Online Bug ID 805277.

**From Data ONTAP 8.3.x**

You can upgrade directly to ONTAP 9.1, then upgrade to later releases.

**From Data ONTAP releases earlier than 8.3.x, including 8.2.x**

You must first upgrade to Data ONTAP 8.3.x, then upgrade to ONTAP 9.1, then upgrade to later releases.

**Verify the LIF failover configuration**

**Related information**

Before you upgrade ONTAP, you must verify that the cluster’s failover policies and
failover groups are configured correctly.

During the upgrade process, LIFs are migrated based on the upgrade method. Depending upon the upgrade method, the LIF failover policy might or might not be used.

If you have 8 or more nodes in your cluster, the automated upgrade is performed using the batch method. The batch upgrade method involves dividing the cluster into multiple upgrade batches, upgrading the set of nodes in the first batch, upgrading their high-availability (HA) partners, and then repeating the process for the remaining batches. In ONTAP 9.7 and earlier, if the batch method is used, LIFs are migrated to the HA partner of the node being upgraded. In ONTAP 9.8 and later, if the batch method is used, LIFs are migrated to the other batch group.

If you have less than 8 nodes in your cluster, the automated upgrade is performed using the rolling method. The rolling upgrade method involves initiating a failover operation on each node in an HA pair, updating the node that has failed over, initiating giveback, and then repeating the process for each HA pair in the cluster. If the rolling method is used, LIFs are migrated to the failover target node as defined by the LIF failover policy.

Steps

1. Display the failover policy for each data LIF:

<table>
<thead>
<tr>
<th>If your ONTAP version is...</th>
<th>Use this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.6 or later</td>
<td>network interface show -service-policy <em>data</em> -failover</td>
</tr>
<tr>
<td>9.5 or earlier</td>
<td>network interface show -role data -failover</td>
</tr>
</tbody>
</table>

This example shows the default failover configuration for a two-node cluster with two data LIFs:
The **Failover Targets** field shows a prioritized list of failover targets for each LIF. For example, if 'lif0' fails over from its home port (e0b on node0), it first attempts to fail over to port e0c on node0. If lif0 cannot fail over to e0c, it then attempts to fail over to port e0d on node0, and so on.

2. If the failover policy is set to **disabled** for any LIFs, other than SAN LIFs, use the `network interface modify` command to enable failover.

3. For each LIF, verify that the **Failover Targets** field includes data ports from a different node that will remain up while the LIF's home node is being upgraded.

You can use the `network interface failover-groups modify` command to add a failover target to the failover group.

**Example**

```
network interface failover-groups modify -vserver vs0 -failover-group fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

**Related information**

- **Network and LIF management**

**Verify SVM routing configuration**

To avoid disruption, before you upgrade your ONTAP software, you should ensure that the default SVM route is able to reach any network address that is not reachable by a
more specific route. It is a best practice to configure one default route for an SVM. For more information, see SU134: Network access might be disrupted by incorrect routing configuration in ONTAP.

The routing table for an SVM determines the network path the SVM uses to communicate with a destination. It’s important to understand how routing tables work so that you can prevent network problems before they occur.

Routing rules are as follows:

• ONTAP routes traffic over the most specific available route.
• ONTAP routes traffic over a default gateway route (having 0 bits of netmask) as a last resort, when more specific routes are not available.

In the case of routes with the same destination, netmask, and metric, there is no guarantee that the system will use the same route after a reboot or after an upgrade. This can especially be an issue if you have configured multiple default routes.

Special considerations

Special considerations prior to an ONTAP upgrade

Certain cluster configurations require you to take specific actions before you begin an ONTAP software upgrade. For example, if you have a SAN configuration, you should verify that each host is configured with the correct number of direct and indirect paths before you begin the upgrade.

Review the following table to determine what additional steps you might need to take.

<table>
<thead>
<tr>
<th>Before you upgrade ONTAP, ask yourself…</th>
<th>If your answer is yes, then do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is my cluster currently in a mixed version state?</td>
<td>Check mixed version requirements</td>
</tr>
<tr>
<td>Do I have a MetroCluster configuration?</td>
<td>Review specific upgrade requirements for MetroCluster configurations</td>
</tr>
<tr>
<td>Do I have a SAN configuration?</td>
<td>Verify the SAN host configuration</td>
</tr>
<tr>
<td>Does my cluster have SnapMirror relationships defined?</td>
<td>Verify compatibility of ONTAP versions for SnapMirror relationships</td>
</tr>
<tr>
<td>Do I have DP-type SnapMirror relationships defined, and am I upgrading to ONTAP 9.12.1 or later?</td>
<td>Convert existing DP-type relationships to XDP</td>
</tr>
<tr>
<td>Am I using NetApp Storage Encryption with external key management servers?</td>
<td>Delete any existing key management server connections</td>
</tr>
<tr>
<td>Do I have netgroups loaded into SVMs?</td>
<td>Verify that the netgroup file is present on each node</td>
</tr>
<tr>
<td>Do I have LDAP clients using SSLv3?</td>
<td>Configure LDAP clients to use TLS</td>
</tr>
<tr>
<td>Am I using session-oriented protocols?</td>
<td>Review considerations for session-oriented protocols</td>
</tr>
<tr>
<td>Is SSL FIPS mode enabled on a cluster where administrator accounts authenticate with an SSH public key?</td>
<td>Verify SSH host key algorithm support</td>
</tr>
</tbody>
</table>
Mixed version ONTAP clusters

A mixed version ONTAP cluster consists of nodes running two different major ONTAP releases for a limited time. For example, if a cluster currently consists of nodes running ONTAP 9.8 and 9.12.1, the cluster is a mixed version cluster. Similarly, a cluster in which nodes are running ONTAP 9.9.1 and 9.13.1 would be a mixed version cluster. NetApp supports mixed version ONTAP clusters for limited periods of time and in specific scenarios.

The following are the most common scenarios in which an ONTAP cluster will be in a mixed version state:

- ONTAP software upgrades in large clusters
- ONTAP software upgrades required when you plan to add new nodes to a cluster

The information applies to ONTAP versions that support NetApp platforms systems, such as AFF A-Series and C-Series, ASA, and FAS, and C-series systems. The information does not apply to ONTAP cloud releases (9.x.0) such as 9.12.0.

Requirements for mixed version ONTAP clusters

If your cluster needs to enter a mixed ONTAP version state, you need to be aware of important requirements and restrictions.

- There cannot be more than two different major ONTAP versions in a cluster at any given time. For example, ONTAP 9.9.1 and 9.13.1 is supported but ONTAP 9.9.1, 9.12.1, and 9.13.1 is not. Clusters that have nodes running with different P or D patch levels of the same ONTAP release, such as ONTAP 9.9.1P1 and 9.9.1P5, are not considered mixed version ONTAP clusters.

- While the cluster is in a mixed version state, you should not enter any commands that alter the cluster operation or configuration except those that are required for the upgrade or data migration process. For example, activities such as (but not limited to) LIF migration, planned storage failover operations, or large-scale object creation or deletion should not be performed until upgrade and data migration are complete.

- For optimal cluster operation, the length of time that the cluster is in a mixed version state should be as short as possible. The maximum length of time a cluster can remain in a mixed version state depends on the lowest ONTAP version in the cluster.

<table>
<thead>
<tr>
<th>If the lowest version of ONTAP running in the mixed version cluster is:</th>
<th>Then you can remain in a mixed version state for a maximum of</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP 9.8 or higher</td>
<td>90 days</td>
</tr>
<tr>
<td>ONTAP 9.7 or lower</td>
<td>7 days</td>
</tr>
</tbody>
</table>

- Beginning with ONTAP 9.8, the version difference between the original nodes and the new nodes cannot be greater than four. For example, a mixed version ONTAP cluster could have nodes running ONTAP 9.8 and 9.12.1, or it could have nodes running ONTAP 9.9.1 and 9.13.1. However, a mixed version ONTAP cluster with nodes running ONTAP 9.8 and 9.13.1 would not be supported.

For a complete list of supported mixed version clusters, see supported upgrade paths. All direct upgrade paths are supported for mixed version clusters.
**Updating the ONTAP version of a large cluster**

One scenario for entering a mixed version cluster state involves upgrading the ONTAP version of a cluster with multiple nodes to take advantage of the features available in later versions of ONTAP 9. When you need to upgrade the ONTAP version of a larger cluster, you will enter a mixed version cluster state for a period of time as you upgrade each node in your cluster.

**Adding new nodes to an ONTAP cluster**

Another scenario for entering a mixed version cluster state involves adding new nodes to your cluster. You might add new nodes to your cluster to expand its capacity, or you might add new nodes as part of the process of completely replacing your controllers. In either case, you need to enable the migration of your data from existing controllers to the new nodes in your new system.

If you plan to add new nodes to your cluster, and those nodes require a minimum version of ONTAP that’s later than the version currently running in your cluster, you need to perform any supported software upgrades on the existing nodes in your cluster before adding the new nodes.

Ideally, you would upgrade all existing nodes to the minimum version of ONTAP required by the nodes you plan to add to the cluster. However, if this is not possible because some of your existing nodes don’t support the later version of ONTAP, you’ll need to enter a mixed version state for a limited amount of time as part of your upgrade process. If you have nodes that do not support the minimum ONTAP version required by your new controllers, you should do the following:

1. **Upgrade** the nodes that do not support the minimum ONTAP version required by your new controllers to the maximum ONTAP version that they do support.

   For example, if you have a FAS8080 running ONTAP 9.5 and you are adding a new C-Series platform running ONTAP 9.12.1, you should upgrade your FAS8080 to ONTAP 9.8 (which is the maximum ONTAP version it supports).

2. **Add the new nodes to your cluster.**

3. **Migrate the data** from the nodes being removed from the cluster to the newly added nodes.

4. **Remove the unsupported nodes from the cluster.**

5. **Upgrade** the remaining nodes in your cluster to the same version as the new nodes.

   Optionally, upgrade the entire cluster (including your new nodes) to the latest recommended patch release of the ONTAP version running on the new nodes.

For details on data migration see:

- Create an aggregate and move volumes to the new nodes
- Setting up new iSCSI connections for SAN volume moves
- Moving volumes with encryption

**ONTAP upgrade requirements for MetroCluster configurations**

Before you upgrade your ONTAP software on a MetroCluster configuration, your clusters must meet certain requirements.

- Both clusters must be running the same version of ONTAP.
You can verify the ONTAP version by using the `version` command.

- If you’re performing a major ONTAP upgrade, the MetroCluster configuration must be in normal mode.
- If you’re performing a patch ONTAP upgrade, the MetroCluster configuration can be in either normal or switchover mode.
- For all configurations except two-node clusters, you can nondisruptively upgrade both clusters at the same time.

For nondisruptive upgrade in two-node clusters, the clusters must be upgraded one node at a time.

- The aggregates in both clusters must not be in resyncing RAID status.

During MetroCluster healing, the mirrored aggregates are resynchronized. You can verify if the MetroCluster configuration is in this state by using the `storage aggregate plex show -in-progress true` command. If any aggregates are being synchronized, you should not perform an upgrade until the resynchronization is complete.

- Negotiated switchover operations will fail while the upgrade is in progress.

To avoid issues with upgrade or revert operations, do not attempt an unplanned switchover during an upgrade or revert operation unless all nodes on both clusters are running the same version of ONTAP.

**Configuration requirements for MetroCluster normal operation**

- The source SVM LIFs must be up and located on their home nodes.

  Data LIFs for the destination SVMs are not required to be up or to be on their home nodes.

- All aggregates at the local site must be online.
- All root and data volumes owned by the local cluster’s SVMs must be online.

**Configuration requirements for MetroCluster switchover**

- All LIFs must be up and located on their home nodes.
- All aggregates must be online, except for the root aggregates at the DR site.

  Root aggregates at the DR site are offline during certain phases of switchover.

- All volumes must be online.

**Related information**

*Verifying networking and storage status for MetroCluster configurations*

**Verify SAN host configuration before an ONTAP upgrade**

Upgrading ONTAP in a SAN environment changes which paths are direct. Before you upgrade a SAN cluster, you should verify that each host is configured with the correct number of direct and indirect paths, and that each host is connected to the correct LIFs.

**Steps**

1. On each host, verify that a sufficient number of direct and indirect paths are configured, and that each path is active.
Each host must have a path to each node in the cluster.

2. Verify that each host is connected to a LIF on each node.

You should record the list of initiators for comparison after the upgrade.

<table>
<thead>
<tr>
<th>For…</th>
<th>Enter…</th>
</tr>
</thead>
<tbody>
<tr>
<td>iSCSI</td>
<td><code>iscsi initiator show -fields igroup,initiator-name,tpgroup</code></td>
</tr>
<tr>
<td>FC</td>
<td><code>fcp initiator show -fields igroup,wwpn,lif</code></td>
</tr>
</tbody>
</table>

**SnapMirror**

**Compatible ONTAP versions for SnapMirror relationships**

The source and destination volumes must be running compatible ONTAP versions before creating a SnapMirror data protection relationship. Before you upgrade ONTAP, you should verify that your current ONTAP version is compatible with your target ONTAP version for SnapMirror relationships.

**Unified replication relationships**

For SnapMirror relationships of type “XDP”, using on premises or Cloud Volumes ONTAP releases:

- **Beginning with ONTAP 9.9.0:**
  
  - ONTAP 9.x.0 releases are cloud-only releases and support Cloud Volumes ONTAP systems. The asterisk (*) after the release version indicates a cloud-only release.
  
  - ONTAP 9.x.1 releases are general releases and support both on-premises and Cloud Volumes ONTAP systems.

  Interoperability is bidirectional.

**Interoperability for ONTAP version 9.3 and later**

<table>
<thead>
<tr>
<th>ONTAP version…</th>
<th>Interoperates with these previous ONTAP versions…</th>
</tr>
</thead>
<tbody>
<tr>
<td>---------------</td>
<td>--------</td>
</tr>
<tr>
<td>SnapMirror Synchronous is not supported for ONTAP cloud instances.</td>
<td></td>
</tr>
</tbody>
</table>

**SnapMirror Synchronous relationships**

*Interoperates with these previous ONTAP versions...*
SnapMirror SVM disaster recovery relationships

- For SVM disaster recovery data and SVM protection:

  SVM disaster recovery is supported only between clusters running the same version of ONTAP. **Version-independence is not supported for SVM replication.**

- For SVM disaster recovery for SVM migration:
  - Replication is supported in a single direction from an earlier version of ONTAP on the source to the same or later version of ONTAP on the destination.
  - The ONTAP version on the target cluster must be no more than two major on-premises versions newer or two major cloud versions newer, as shown in the table below.
    - Replication is not supported for long-term data protection use cases.

The asterisk (*) after the release version indicates a cloud-only release.

To determine support, locate the source version in the left table column, and then locate the destination version on the top row (DR/Migration for like versions and Migration only for newer versions).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---------------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.6</td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.7</td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.8</td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.9.0*</td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.9.1</td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.10.0*</td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.10.1</td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.11.0*</td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.11.1</td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.12.0*</td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.12.1</td>
<td></td>
<td>DR/ Migration</td>
<td>Migration</td>
<td>Migration</td>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SnapMirror disaster recovery relationships

For SnapMirror relationships of type “DP” and policy type “async-mirror”:

− DP-type mirrors cannot be initialized beginning with ONTAP 9.11.1 and are completely deprecated in ONTAP 9.12.1. For more information, see Deprecation of data protection SnapMirror relationships.

− In the following table, the column on the left indicates the ONTAP version on the source volume, and the top row indicates the ONTAP versions you can have on your destination volume.

<table>
<thead>
<tr>
<th>Source</th>
<th>9.11.1</th>
<th>9.10.1</th>
<th>9.9.1</th>
<th>9.8</th>
<th>9.7</th>
<th>9.6</th>
<th>9.5</th>
<th>9.4</th>
<th>9.3</th>
<th>9.2</th>
<th>9.1</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.11.1</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9.10.1</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9.9.1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9.8</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9.7</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9.6</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9.5</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9.4</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9.3</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9.2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9.1</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>9</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Interoperability is not bidirectional.

Convert an existing DP-type relationship to XDP

If you are upgrading to ONTAP 9.12.1 or later, you must convert DP-type relationships to XDP before upgrading. ONTAP 9.12.1 and later does not support DP-type relationships. You can easily convert an existing DP-type relationship to XDP to take advantage of version-flexible SnapMirror.

About this task

• SnapMirror does not automatically convert existing DP-type relationships to XDP. To convert the relationship, you need to break and delete the existing relationship, create a new XDP relationship, and resync the relationship. For background information, see XDP replaces DP as the SnapMirror default.

• When planning your conversion, you should be aware that background preparation and the data warehousing phase of an XDP SnapMirror relationship can take a long time. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

After you convert a SnapMirror relationship type from DP to XDP, space-related settings, such as autosize and space guarantee are no longer replicated to the destination.

Steps

1. From the destination cluster, ensure that the SnapMirror relationship is type DP, that the mirror state is SnapMirrored, the relationship status is Idle, and the relationship is healthy:

   snapmirror show -destination-path <SVM:volume>

   The following example shows the output from the snapmirror show command:
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true

You might find it helpful to retain a copy of the `snapmirror show` command output to keep track existing of the relationship settings.

2. From the source and the destination volumes, ensure that both volumes have a common Snapshot copy:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

The following example shows the `volume snapshot show` output for the source and the destination volumes:
cluster_src:> volume snapshot show -vserver vsml -volume volA

---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------- -------- --------
------ -----
sml volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-27_100026
valid 44KB 0% 19%
11 entries were displayed.

cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst

---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------- -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-27_100026
valid 44KB 0% 19%

3. To ensure scheduled updates will not run during the conversion, quiesce the existing DP-type relationship:
snapmirror quiesce -source-path <SVM:volume> -destination-path <SVM:volume>

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

The following example quiesces the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

4. Break the existing DP-type relationship:

```
snapmirror break -destination-path <SVM:volume>
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

The following example breaks the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

5. If automatic deletion of Snapshot copies is enabled on the destination volume, disable it:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_ -enabled false
```

The following example disables Snapshot copy autodelete on the destination volume `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup -volume volA_dst -enabled false
```

6. Delete the existing DP-type relationship:

```
snapmirror delete -destination-path <SVM:volume>
```

For complete command syntax, see the man page.
You must run this command from the destination SVM or the destination cluster.

The following example deletes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Release the origin SVM disaster recovery relationship on the source:

```
snapmirror release -destination-path <SVM:volume> -relationship-info-only true
```

The following example releases the SVM disaster recovery relationship:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
```

8. You can use the output you retained from the `snapmirror show` command to create the new XDP-type relationship:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type XDP -schedule <schedule> -policy <policy>
```

The new relationship must use the same source and destination volume. For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

The following example creates a SnapMirror disaster recovery relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup` using the default `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination-path
svm_backup:volA_dst -type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Resync the source and destination volumes:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```
To improve resync time, you can use the `-quick-resync` option, but you should be aware that storage efficiency savings can be lost. For complete command syntax, see the man page: SnapMirror resync command.

You must run this command from the destination SVM or the destination cluster. Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

The following example resyncs the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination-path svm_backup:volA_dst
```

10. If you disabled automatic deletion of Snapshot copies, reenable it:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume> -enabled true
```

After you finish

1. Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

2. Once the SnapMirror XDP destination volume begins updating Snapshot copies as defined by the SnapMirror policy, use the output of `snapmirror list-destinations` command from the source cluster to display the new SnapMirror XDP relationship.

Delete existing external key management server connections before upgrading ONTAP

Before you upgrade ONTAP, if you are running ONTAP 9.2 or earlier with NetApp Storage Encryption (NSE) and upgrading to ONTAP 9.3 or later, you must use the command line interface (CLI) to delete any existing external key management (KMIP) server connections.

Steps

1. Verify that the NSE drives are unlocked, open, and set to the default manufacture secure ID 0x0:

   ```
   storage encryption disk show -disk *
   ```

2. Enter the advanced privilege mode:

   ```
   set -privilege advanced
   ```

3. Use the default manufacture secure ID 0x0 to assign the FIPS key to the self-encrypting disks (SEDs):
4. Verify that assigning the FIPS key to all disks is complete:

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

5. Verify that the mode for all disks is set to data

```
storage encryption disk show-status
```

6. View the configured KMIP servers:

```
security key-manager show
```

7. Delete the configured KMIP servers:

```
security key-manager delete -address kmip_ip_address
```

8. Delete the external key manager configuration:

```
security key-manager delete-kmip-config
```

This step does not remove the NSE certificates.

**What’s next**

After the upgrade is complete, you must reconfigure the KMIP server connections.

**Verify netgroup file is present on all nodes before an ONTAP upgrade**

Before you upgrade ONTAP, if you have loaded netgroups into storage virtual machines (SVMs), you must verify that the netgroup file is present on each node. A missing netgroup file on a node can cause an upgrade to fail.

**Steps**

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Display the netgroup status for each SVM:
3. Verify that for each SVM, each node shows the same netgroup file hash value:

```
vserver services name-service netgroup status
```

If this is the case, you can skip the next step and proceed with the upgrade or revert. Otherwise, proceed to the next step.

4. On any one node of the cluster, manually load the netgroup file:

```
vserver services netgroup load -vserver vserver_name -source uri
```

This command downloads the netgroup file on all nodes. If a netgroup file already exists on a node, it is overwritten.

**Related information**

**Working with Netgroups**

**Configure LDAP clients to use TLS for highest security**

Before you upgrade ONTAP, you must configure LDAP clients using SSLv3 for secure communications with LDAP servers to use TLS. SSL will not be available after the upgrade.

By default, LDAP communications between client and server applications are not encrypted. You must disallow the use of SSL and enforce the use of TLS.

**Steps**

1. Verify that the LDAP servers in your environment support TLS.

   If they do not, do not proceed. You should upgrade your LDAP servers to a version that supports TLS.

2. Check which ONTAP LDAP client configurations have LDAP over SSL/TLS enabled:

   ```
vserver services name-service ldap client show
   ```

   If there are none, you can skip the remaining steps. However, you should consider using LDAP over TLS for better security.

3. For each LDAP client configuration, disallow SSL to enforce the use of TLS:

   ```
vserver services name-service ldap client modify -vserver vserver_name -client-config ldap_client_config_name -allow-ssl false
   ```
4. Verify that the use of SSL is no longer allowed for any LDAP clients:

```
vserver services name-service ldap client show
```

### Related information

**NFS management**

### Considerations for session-oriented protocols

Clusters and session-oriented protocols might cause adverse effects on clients and applications in certain areas such as I/O service during upgrades.

If you are using session-oriented protocols, consider the following:

- **SMB**

  If you serve continuously available (CA) shares with SMBv3, you can use the automated nondisruptive upgrade method (with System Manager or the CLI), and no disruption is experienced by the client.

  If you are serving shares with SMBv1 or SMBv2, or non-CA shares with SMBv3, client sessions are disrupted during upgrade takeover and reboot operations. You should direct users to end their sessions before you upgrade.

  Hyper-V and SQL Server over SMB support nondisruptive operations (NDOs). If you configured a Hyper-V or SQL Server over SMB solution, the application servers and the contained virtual machines or databases remain online and provide continuous availability during the ONTAP upgrade.

- **NFSv4.x**

  NFSv4.x clients will automatically recover from connection losses experienced during the upgrade using normal NFSv4.x recovery procedures. Applications might experience a temporary I/O delay during this process.

- **NDMP**

  State is lost and the client user must retry the operation.

- **Backups and restores**

  State is lost and the client user must retry the operation.

  Do not initiate a backup or restore during or immediately before an upgrade. Doing so might result in data loss.

- **Applications (for example, Oracle or Exchange)**

  Effects depend on the applications. For timeout-based applications, you might be able to change the timeout setting to longer than the ONTAP reboot time to minimize adverse effects.
Verify SSH host key algorithm support before ONTAP upgrade

Before you upgrade ONTAP, if SSL FIPS mode is enabled on a cluster where administrator accounts authenticate with an SSH public key, you must ensure that the host key algorithm is supported on the target ONTAP release.

The following table indicates host key type algorithms that are supported for ONTAP SSH connections. These key types do not apply to configuring SSH public authentication.

<table>
<thead>
<tr>
<th>ONTAP release</th>
<th>Key types supported in FIPS mode</th>
<th>Key types supported in non-FIPS mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.11.1 and later</td>
<td>ecdsa-sha2-nistp256</td>
<td>ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa</td>
</tr>
<tr>
<td></td>
<td>ssh-ed25519</td>
<td>ssh-ed25519 ssh-dss ssh-rsa</td>
</tr>
</tbody>
</table>

Support for the ssh-ed25519 host key algorithm is removed beginning with ONTAP 9.11.1.

For more information, see Configure network security using FIPS.

Existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type before upgrading or administrator authentication will fail.

Learn more about enabling SSH public key accounts.

Reboot SP or BMC to prepare for firmware update during an ONTAP upgrade

You do not need to manually update your firmware prior to an ONTAP upgrade. The firmware for your cluster is included with the ONTAP upgrade package and is copied to each node’s boot device. The new firmware is then installed as part of the upgrade process.

Firmware for the following components is updated automatically if the version in your cluster is older than the firmware that is bundled with the ONTAP upgrade package:

- BIOS/LOADER
- Service Processor (SP) or baseboard management controller (BMC)
- Storage shelf
- Disk
- Flash Cache

To prepare for a smooth update, you should reboot the SP or BMC before the upgrade begins.
Step

1. Reboot the SP or BMC prior to the upgrade:

   ```
   system service-processor reboot-sp -node node_name
   ```

   Only reboot one SP or BMC at a time. Wait for the rebooted SP or BMC to completely recycle before rebooting the next.

You can also update firmware manually in between ONTAP upgrades. If you have Active IQ, you can view the list of firmware versions currently included in your ONTAP image.

Updated firmware versions are available as follows:

- System firmware (BIOS, BMC, SP)
- Shelf firmware
- Disk and Flash Cache firmware

**Download the ONTAP software image**

Before you upgrade ONTAP, you must first download the target ONTAP software image from the NetApp Support site. Depending on your ONTAP release, you can download the ONTAP software to an HTTPS, HTTP or FTP server on your network, or to a local folder.

<table>
<thead>
<tr>
<th>If you are running...</th>
<th>You can download the image to this location...</th>
</tr>
</thead>
</table>
| ONTAP 9.6 and later    | • An HTTPS server  
                          The server’s CA certificate must be installed on the local system.  
                          • A local folder  
                          • An HTTP or FTP server |
| ONTAP 9.4 and later    | • A local folder  
                          • An HTTP or FTP server |
| ONTAP 9.0 and later    | An HTTP or FTP server |

**About this task**

- If you are performing an automated nondisruptive upgrade (ANDU) using a direct multi-hop upgrade path, you need to download the software package for both the intermediate ONTAP version and the target ONTAP version required for your upgrade. For example, if you are upgrading from ONTAP 9.8 to ONTAP 9.13.1, you must download the software packages for both ONTAP 9.12.1 and ONTAP 9.13.1. See supported upgrade paths to determine if your upgrade path requires you to download an intermediate software package.

- If you are upgrading a system with NetApp Volume Encryption to ONTAP 9.5 or later, you must download the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.
If you use the ONTAP software image for restricted countries to upgrade a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

- You do not need to download a separate software package for your firmware. The firmware update for your cluster is included with the ONTAP software upgrade package and is copied to each node’s boot device. The new firmware is then installed as part of the upgrade process.

Steps
1. Locate the target ONTAP software in the Software Downloads area of the NetApp Support Site.
   - For an ONTAP Select upgrade, select ONTAP Select Node Upgrade.
2. Copy the software image (for example, 97_q_image.tgz) to the appropriate location.
   - Depending on your ONTAP release, the location will be a directory an HTTP, HTTPS or FTP server from which the image will be served to the local system, or to a local folder on the storage system.

ONTAP upgrade methods

ONTAP software upgrade methods

You can perform an automated upgrade of your ONTAP software using System Manager. Alternately, you can perform an automated or manual upgrade using the ONTAP command line interface (CLI). The method you use to upgrade ONTAP depends upon your configuration, your current ONTAP version, and the number of nodes in your cluster. NetApp recommends using System Manager to perform automated upgrades unless your configuration requires a different approach. For example, if you have a MetroCluster configuration with 4 nodes running ONTAP 9.3 or later, you should use System Manager to perform an automated upgrade (sometimes referred to as automated nondisruptive upgrade or ANDU). If you have a MetroCluster configuration with 8 nodes running ONTAP 9.2 or earlier, you should use the CLI to perform a manual upgrade.

An upgrade can be executed using the rolling upgrade process or the batch upgrade process. Both are nondisruptive.

ONTAP rolling upgrades

In the rolling upgrade process, a node is taken offline and upgraded while its partner takes over its storage. When the node upgrade is complete, the partner node gives control back to the original owning node, and the process is repeated on the partner node. Each additional HA pair is upgraded in sequence until all HA pairs are running the target release. The rolling upgrade process is the default for clusters with fewer than 8 nodes.

ONTAP batch upgrades

In the batch upgrade process, the cluster is divided into several batches, each of which contains multiple HA pairs. In the first batch, one node of each HA pair is upgraded, followed by their HA partners. The process is then repeated sequentially for the remaining batches. The batch upgrade process is the default for clusters of 8 nodes or more.

For automated upgrades, ONTAP automatically installs the target ONTAP image on each node, validates the cluster components to ensure that the cluster can be upgraded nondisruptively, and then executes a batch or rolling upgrade in the background based on the number of nodes. For manual upgrades, the administrator manually confirms that each node in the cluster is ready for upgrade, then performs steps to execute a rolling
Recommended ONTAP upgrade methods based on configuration

Upgrade methods supported by your configuration are listed in order of recommended usage.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>ONTAP version</th>
<th>Number of nodes</th>
<th>Recommended upgrade method</th>
</tr>
</thead>
</table>
| Standard      | 9.0 or later  | 2 or more       | • Automated nondisruptive using System Manager  
                 |               |                 | • Automated nondisruptive using the CLI  |
| Standard      | 9.0 or later  | Single          | Automated disruptive      |
| MetroCluster  | 9.3 or later  | 8               | • Automated nondisruptive using the CLI  
                 |               |                 | • Manual nondisruptive for 4 or 8 node MetroCluster using the CLI  |
| MetroCluster  | 9.3 or later  | 2,4             | • Automated nondisruptive using System Manager  
                 |               |                 | • Automated nondisruptive using the CLI  |
| MetroCluster  | 9.2 or earlier| 4, 8            | Manual nondisruptive for 4 or 8 node MetroCluster using the CLI  |
| MetroCluster  | 9.2 or earlier| 2               | Manual nondisruptive for 2-node MetroCluster using the CLI  |

ANDU using System Manager is the recommended upgrade method for all patch upgrades regardless of configuration.

A manual disruptive upgrade can be performed on any configuration. However, you should not perform a disruptive upgrade unless you can take the cluster offline for the duration of the upgrade. If you are operating in a SAN environment, you should be prepared to shut down or suspend all SAN clients before performing a disruptive upgrade. Disruptive upgrades are performed using the ONTAP CLI.
Automated upgrades

Automated nondisruptive ONTAP upgrade

When you perform an automated upgrade, ONTAP automatically installs the target ONTAP image on each node, validates that the cluster can be upgraded successfully, and then executes either a batch or rolling upgrade in the background based on the number of nodes in the cluster.

If it is supported by your configuration, you should use System Manager to perform an automated upgrade. If your configuration does not support automated upgrade using System Manager, you can use the ONTAP command line interface (CLI) to perform an automated upgrade.

Before you begin

- You should prepare for your upgrade.
- You should download the ONTAP software image for your target ONTAP release.

If you are performing a direct multi-hop upgrade, you need to download both of the ONTAP images required for your specific upgrade path.

- For each HA pair, each node should have one or more ports on the same broadcast domain.

If you have 8 or more nodes, the batch upgrade method is used in the automatic nondisruptive upgrade. In ONTAP 9.7 and earlier, if the batch method is used, LIFs are migrated to the HA partner of the node being upgraded. If the partners don’t have any ports in the same broadcast domain, then the LIF migration fails.

In ONTAP 9.8 and later, if the batch method is used, LIFs are migrated to the other batch group.

- If you are upgrading ONTAP in a MetroCluster FC configuration, the cluster should be enabled for automatic unplanned switchover.
- If you don’t plan to monitor the progress of the upgrade process, you should request EMS notifications of errors that might require manual intervention.
Example 2. Steps

**System Manager**

1. Validate the ONTAP target image:

   ![Tip]

   If you are upgrading a MetroCluster configuration, you should validate Cluster A and then repeat the validation process on Cluster B.

   a. Depending on the ONTAP version that you are running, perform one of the following steps:

<table>
<thead>
<tr>
<th>If you are running...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP 9.8 or later</td>
<td>Click Cluster &gt; Overview.</td>
</tr>
<tr>
<td>ONTAP 9.5, 9.6, and 9.7</td>
<td>Click Configuration &gt; Cluster &gt; Update.</td>
</tr>
<tr>
<td>ONTAP 9.4 or earlier</td>
<td>Click Configuration &gt; Cluster Update.</td>
</tr>
</tbody>
</table>

   b. In the right corner of the **Overview** pane, click ⚒.

   c. Click **ONTAP Update**.

   d. In the **Cluster Update** tab, add a new image or select an available image.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
</table>
   | Add a new software image from a local folder | i. Under **Available Software Images**, click **Add from Local**.  
   | You should have already downloaded the image to the local client. | ii. Browse to the location you saved the software image, select the image, and then click **Open**. |
   | Add a new software image from an HTTP or FTP server | i. Click **Add from Server**.  
   | | ii. In the **Add a New Software Image** dialog box, enter the URL of the HTTP or FTP server to which you downloaded the ONTAP software image from the NetApp Support Site.  
   | | For anonymous FTP, you must specify the URL in the **ftp://anonymous@ftpserver** format.  
   | | iii. Click **Add**. |
   | Select an available image | Choose one of the listed images. |

   e. Click **Validate** to run the pre-upgrade validation checks.

   If any errors or warnings are found during validation, they are displayed along with a list of corrective actions. You must resolve all errors before proceeding with the upgrade. It is best
practice to also resolve warnings.

2. Click **Next**.
3. Click **Update**.

Validation is performed again. Any remaining errors or warnings are displayed along with a list of corrective actions. Errors must be corrected before you can proceed with the upgrade. If the validation is completed with warnings, you correct the warnings or choose **Update with warnings**.

By default, ONTAP uses the **batch upgrade process** to upgrade clusters with eight or more nodes. Beginning in ONTAP 9.10.1, if preferred, you can select **Update one HA pair at a time** to override the default and have your cluster upgrade one HA pair at a time using the rolling upgrade process.

For MetroCluster configurations with more than 2 nodes, the ONTAP upgrade process starts simultaneously on the HA pairs at both sites. For a 2-node MetroCluster configuration, the upgrade is started first on the site where the upgrade is not initiated. The upgrade on the remaining site begins after the first upgrade is fully completed.

4. If your upgrade pauses because of an error, click the error message to view the details, then correct the error and **resume the upgrade**.

**After you finish**

After the upgrade is completed successfully, the node reboots, and you are redirected to the System Manager login page. If the node takes a long time to reboot, you should refresh your browser.

**CLI**

1. Validate the ONTAP target software image

If you are upgrading a MetroCluster configuration you should first execute the following steps on cluster A, then execute the same steps on cluster B.

a. Delete the previous ONTAP software package:

```
cluster image package delete -version previous_ONTAP_Version
```

b. Load the target ONTAP software image into the cluster package repository:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url

Package download completed.
Package processing completed.
```

If you are performing a **direct multi-hop upgrade**, you also need to load the software package for
the intermediate version of ONTAP required for your upgrade. For example, if you are upgrading from 9.8 to 9.13.1, you need to load the software package for ONTAP 9.12.1, and then use the same command to load the software package for 9.13.1.

c. Verify that the software package is available in the cluster package repository:

```
ccluster image package show-repository

cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
 9.13.1           MM/DD/YYYY 10:32:15
```

d. Execute the automated pre-upgrade checks:

```
ccluster image validate -version package_version_number

If you are performing a direct multi-hop upgrade, you only need to use the target ONTAP package for verification. You don’t need to validate the intermediate upgrade image separately. For example, if you are upgrading from 9.8 to 9.13.1, use the 9.13.1 package for verification. You don’t need to validate the 9.12.1 package separately.

cluster1::> cluster image validate -version 9.13.1

WARNING: There are additional manual upgrade validation checks that must be performed after these automated validation checks have completed...
```

e. Monitor the progress of the validation:

```
ccluster image show-update-progress
```

f. Complete all required actions identified by the validation.

g. If you are upgrading a MetroCluster configuration, repeat the above steps on cluster B.

2. Generate a software upgrade estimate:

```
ccluster image update -version package_version_number -estimate-only

If you are upgrading a MetroCluster configuration, you can run this command on either Cluster A or Cluster B. You don’t need to run it on both clusters.
The software upgrade estimate displays details about each component to be updated, as well as the estimated duration of the upgrade.

3. Perform the software upgrade:

```
cluster image update -version package_version_number
```

- If you are performing a **direct multi-hop upgrade**, use the target ONTAP version for the `package_version_number`. For example, if you are upgrading from ONTAP 9.8 to 9.13.1, use 9.13.1 as the `package_version_number`.

- By default, ONTAP uses the **batch upgrade process** to upgrade clusters with eight or more nodes. If preferred, you can use the `-force-rolling` parameter to override the default process and have your cluster upgraded one node at a time using the rolling upgrade process.

- After completing each takeover and giveback, the upgrade waits for 8 minutes to enable client applications to recover from the pause in I/O that occurs during the takeover and giveback. If your environment requires more or less time for client stabilization, you can use the `-stabilize -minutes` parameter to specify a different amount of stabilization time.

- For MetroCluster configurations with 4 nodes more, the automated upgrade starts simultaneously on the HA pairs at both sites. For a 2-node MetroCluster configuration, the upgrade starts on the site where the upgrade is not initiated. The upgrade on the remaining site begins after the first upgrade is fully completed.

```
cluster1::> cluster image update -version 9.13.1
Starting validation for this update. Please wait..
It can take several minutes to complete validation...
WARNING: There are additional manual upgrade validation checks...
Pre-update Check Status Error-Action
------------------------------- -------
...                                                         
20 entries were displayed
Would you like to proceed with update ? {y|n}: y
Starting update...
cluster-1:>
```

4. Display the cluster update progress:

```
cluster image show-update-progress
```
If you are upgrading a 4-node or 8-node MetroCluster configuration, the `cluster image show-update-progress` command only displays the progress for the node on which you run the command. You must run the command on each node to see individual node progress.

5. Verify that the upgrade was completed successfully on each node.

```
cluster image show-update-progress
```

```
cluster1::> cluster image show-update-progress

Estimated  
Elapsed    
Update Phase Status             Duration  
Duration   
----------------- ----------------- --------------- 
---------------
Pre-update checks completed            00:10:00   
00:02:07
Data ONTAP updates completed            01:31:00   
01:39:00
Post-update checks completed            00:10:00   
00:02:00
3 entries were displayed.

Updated nodes: node0, node1.
```

6. Trigger an AutoSupport notification:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

If your cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

7. If you are upgrading a 2-node MetroCluster FC configuration, verify that the cluster is enabled for automatic unplanned switchover.

```
If you are upgrading a standard configuration, a MetroCluster IP configuration, or a MetroCluster FC configuration greater than 2 nodes, you don’t need to perform this step.
```

a. Check whether automatic unplanned switchover is enabled:

```
microcluster show
```
If automatic unplanned switchover is enabled, the following statement appears in the command output:

```
AUSO Failure Domain auso-on-cluster-disaster
```

b. If the statement does not appear in the output, enable automatic unplanned switchover:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster
```

c. Verify that automatic unplanned switchover has been enabled:

```
metrocluster show
```

**Video: Upgrades made easy**

Take a look at the simplified ONTAP upgrade capabilities of System Manager in ONTAP 9.8.

---

**Related information**

- Launch Active IQ
- Active IQ documentation
Automated disruptive ONTAP upgrade (single-node cluster only)

Beginning with ONTAP 9.2, you can use the ONTAP CLI to perform an automated update of a single-node cluster. Because single-node clusters lack redundancy, updates are always disruptive. Disruptive upgrades cannot be performed using System Manager.

- You must have satisfied upgrade preparation requirements.

Steps

1. Delete the previous ONTAP software package:

   ```bash
   cluster image package delete -version previous_package_version
   ```

2. Download the target ONTAP software package:

   ```bash
   cluster image package get -url location
   ```

   ```bash
   cluster1::> cluster image package get -url
   http://www.example.com/software/9.7/image.tgz
   ```

   Package download completed.
   Package processing completed.

3. Verify that the software package is available in the cluster package repository:

   ```bash
   cluster image package show-repository
   ```

   ```bash
   cluster1::> cluster image package show-repository
   Package Version   Package Build Time
   ----------------- ------------------
   9.7              M/DD/YYYY 10:32:15
   ```

4. Verify that the cluster is ready to be upgraded:

   ```bash
   cluster image validate -version package_version_number
   ```

   ```bash
   cluster1::> cluster image validate -version 9.7
   WARNING: There are additional manual upgrade validation checks that must be performed after these automated validation checks have completed...```
5. Monitor the progress of the validation:

```
cluster image show-update-progress
```

6. Complete all required actions identified by the validation.

7. Optionally, generate a software upgrade estimate:

```
cluster image update -version package_version_number -estimate-only
```

The software upgrade estimate displays details about each component to be updated, and the estimated duration of the upgrade.

8. Perform the software upgrade:

```
cluster image update -version package_version_number
```

If an issue is encountered, the update pauses and prompts you to take corrective action. You can use the `cluster image show-update-progress` command to view details about any issues and the progress of the update. After correcting the issue, you can resume the update by using the `cluster image resume-update` command.

9. Display the cluster update progress:

```
cluster image show-update-progress
```

The node is rebooted as part of the update and cannot be accessed while rebooting.

10. Trigger a notification:

```
autosupport invoke -node * -type all -message "Finishing Upgrade"
```

If your cluster is not configured to send messages, a copy of the notification is saved locally.

**Resume ONTAP software upgrade after an error in the automated upgrade process**

If an automated ONTAP software upgrade pauses because of an error, you should resolve the error and then continue the upgrade. After the error is resolved, you can choose to continue the automated upgrade process or complete the upgrade process manually. If you choose to continue the automated upgrade, don’t perform any of the upgrade steps manually.
Example 3. Steps

System Manager
1. Depending on the ONTAP version that you are running, perform one of the following steps:

<table>
<thead>
<tr>
<th>If you are running...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP 9.8 or later</td>
<td>Click <strong>Cluster &gt; Overview</strong></td>
</tr>
<tr>
<td>ONTAP 9.7, 9.6, or 9.5</td>
<td>Click <strong>Configuration &gt; Cluster &gt; Update</strong>.</td>
</tr>
</tbody>
</table>
| ONTAP 9.4 or earlier  | • Click **Configuration > Cluster Update**.  
|                      | • In the right corner of the **Overview** pane, click the three blue vertical dots, and select **ONTAP Update**. |

2. Continue the automated upgrade or cancel it and continue manually.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resume the automated upgrade</td>
<td>Click <strong>Resume</strong>.</td>
</tr>
<tr>
<td>Cancel the automated upgrade and continue manually</td>
<td>Click <strong>Cancel</strong>.</td>
</tr>
</tbody>
</table>

CLI
1. View the upgrade error:

   ```
   cluster image show-update-progress
   ```

2. Resolve the error.
3. Resume the upgrade:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter the following command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resume the automated upgrade</td>
<td><code>cluster image resume-update</code></td>
</tr>
<tr>
<td>Cancel the automated upgrade and continue manually</td>
<td><code>cluster image cancel-update</code></td>
</tr>
</tbody>
</table>

After you finish

*Perform post-upgrade checks.*
Manual upgrades

Install the ONTAP software package for manual upgrades

After you have downloaded the ONTAP software package for a manual upgrade, you must install it locally before you begin your upgrade.

Steps

1. Set the privilege level to advanced, entering y when prompted to continue:

   ```
   set -privilege advanced
   ```

   The advanced prompt (*>) appears.

2. Install the image.

<table>
<thead>
<tr>
<th>If you have the following configuration…</th>
<th>Use this command…</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Non-MetroCluster</td>
<td>system node image update -node * -package <em>location</em> -replace -package true -setdefault true -background true</td>
</tr>
<tr>
<td>• 2-node MetroCluster</td>
<td></td>
</tr>
<tr>
<td></td>
<td>location can be a web server or a local folder, depending on the ONTAP version. See the system node image update man page for details.</td>
</tr>
<tr>
<td></td>
<td>This command installs the software image on all of the nodes simultaneously. To install the image on each node one at a time, do not specify the -background parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>• 4-node MetroCluster</td>
<td>system node image update -node * -package location -replace -package true -background true -setdefault false</td>
</tr>
<tr>
<td>• 8-node MetroCluster configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You must issue this command on both clusters.</td>
</tr>
<tr>
<td></td>
<td>This command uses an extended query to change the target software image, which is installed as the alternate image on each node.</td>
</tr>
</tbody>
</table>

3. Enter y to continue when prompted.

4. Verify that the software image is installed on each node.

   ```
   system node image show-update-progress -node *
   ```
This command displays the current status of the software image installation. You should continue to run this command until all nodes report a Run Status of Exited, and an Exit Status of Success.

The system node image update command can fail and display error or warning messages. After resolving any errors or warnings, you can run the command again.

This example shows a two-node cluster in which the software image is installed successfully on both nodes:

```
class1:*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
  Run Status: Exited
  Exit Status: Success
  Phase: Run Script
  Exit Message: After a clean shutdown, image2 will be set as the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
  Run Status: Exited
  Exit Status: Success
  Phase: Run Script
  Exit Message: After a clean shutdown, image2 will be set as the default boot image on node1.
2 entries were acted on.
```

Manual nondisruptive ONTAP upgrade using the CLI (standard configurations)

Automated upgrade using System Manager is the preferred upgrade method. If System Manager does not support your configuration, you can use the ONTAP command line interface (CLI) to perform a manual nondisruptive upgrade. To upgrade a cluster of two or more nodes using the manual nondisruptive method, you must initiate a failover operation on each node in an HA pair, update the “failed” node, initiate giveback, and then repeat the process for each HA pair in the cluster.

Before you begin
You must have satisfied upgrade preparation requirements.

Updating the first node in an HA pair
You can update the first node in an HA pair by initiating a takeover by the node’s partner. The partner serves the node’s data while the first node is upgraded.

If you are performing a major upgrade, the first node to be upgraded must be the same node on which you configured the data LIFs for external connectivity and installed the first ONTAP image.

After upgrading the first node, you should upgrade the partner node as quickly as possible. Do not allow the two nodes to remain in a mixed version state longer than necessary.
Steps

1. Update the first node in the cluster by invoking an AutoSupport message:

   ```bash
   autosupport invoke -node * -type all -message "Starting_NDU"
   ```

   This AutoSupport notification includes a record of the system status just prior to update. It saves useful troubleshooting information in case there is a problem with the update process.

   If the cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

2. Set the privilege level to advanced, entering `y` when prompted to continue:

   ```bash
   set -privilege advanced
   ```

   The advanced prompt (*>>) appears.

3. Set the new ONTAP software image to be the default image:

   ```bash
   system image modify {-node nodenameA -iscurrent false} -isdefault true
   ```

   The system image modify command uses an extended query to change the new ONTAP software image (which is installed as the alternate image) to the default image for the node.

4. Monitor the progress of the update:

   ```bash
   system node upgrade-revert show
   ```

5. Verify that the new ONTAP software image is set as the default image:

   ```bash
   system image show
   ```

   In the following example, image2 is the new ONTAP version and is set as the default image on node0:
cluster1::*> system image show

<table>
<thead>
<tr>
<th>Node</th>
<th>Image</th>
<th>Default</th>
<th>Current</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>image1</td>
<td>false</td>
<td>true</td>
<td>X.X.X</td>
<td>MM/DD/YYYY TIME</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>Y.Y.Y</td>
<td>MM/DD/YYYY TIME</td>
</tr>
</tbody>
</table>

node1

<table>
<thead>
<tr>
<th>Image</th>
<th>Default</th>
<th>Current</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>image1</td>
<td>true</td>
<td>true</td>
<td>X.X.X</td>
<td>MM/DD/YYYY TIME</td>
</tr>
<tr>
<td>image2</td>
<td>false</td>
<td>false</td>
<td>Y.Y.Y</td>
<td>MM/DD/YYYY TIME</td>
</tr>
</tbody>
</table>

4 entries were displayed.

6. Disable automatic giveback on the partner node if it is enabled:

```
storage failover modify -node nodenameB -auto-giveback false
```

If the cluster is a two-node cluster, a message is displayed warning you that disabling automatic giveback prevents the management cluster services from going online in the event of an alternating-failure scenario. Enter `y` to continue.

7. Verify that automatic giveback is disabled for node's partner:

```
storage failover show -node nodenameB -fields auto-giveback
```

```
ccluster1::> storage failover show -node node1 -fields auto-giveback
node  auto-giveback
-------  ----------
node1    false
1 entry was displayed.
```

8. Run the following command twice to determine whether the node to be updated is currently serving any clients

```
system node run -node nodenameA -command uptime
```

The uptime command displays the total number of operations that the node has performed for NFS, SMB, FC, and iSCSI clients since the node was last booted. For each protocol, you must run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.
You should make a note of each protocol that has increasing client operations so that after the node is updated, you can verify that client traffic has resumed.

The following example shows a node with NFS, SMB, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```sh
cluster1::> system node run -node node0 -command uptime
  2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
  2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP ops, 40395 FCP ops, 32815 iSCSI ops
```

9. Migrate all of the data LIFs away from the node:

```sh
network interface migrate-all -node nodenameA
```

10. Verify any LIFs that you migrated:

```sh
network interface show
```

For more information about parameters you can use to verify LIF status, see the network interface show man page.

The following example shows that node0's data LIFs migrated successfully. For each LIF, the fields included in this example enable you to verify the LIF's home node and port, the current node and port to which the LIF migrated, and the LIF's operational and administrative status.

```sh
cluster1::> network interface show -data-protocol nfs|cifs -role data -home-node node0 -fields home-node,curr-node,curr-port,home-port,status-admin,status-oper
vserver lif  home-node home-port curr-node curr-port status-oper
status-admin
------------ ------------- ------------- --------- ---------- ----------
vs0  data001 node0  e0a  node1  e0a  up   up
vs0  data002 node0  e0b  node1  e0b  up   up
vs0  data003 node0  e0b  node1  e0b  up   up
vs0  data004 node0  e0a  node1  e0a  up   up
4 entries were displayed.
```

11. Initiate a takeover:
storage failover takeover -ofnode nodenameA

Do not specify the -option immediate parameter, because a normal takeover is required for the node that is being taken over to boot onto the new software image. If you did not manually migrate the LIFs away from the node, they automatically migrate to the node’s HA partner to ensure that there are no service disruptions.

The first node boots up to the Waiting for giveback state.

If AutoSupport is enabled, an AutoSupport message is sent indicating that the node is out of cluster quorum. You can ignore this notification and proceed with the update.

12. Verify that the takeover is successful:

storage failover show

You might see error messages indicating version mismatch and mailbox format problems. This is expected behavior and it represents a temporary state in a major nondisruptive upgrade and is not harmful.

The following example shows that the takeover was successful. Node node0 is in the Waiting for giveback state, and its partner is in the In takeover state.

```
cluster1::> storage failover show

+------------------------------------------------------------------------------+
<table>
<thead>
<tr>
<th>Node</th>
<th>Partner</th>
<th>Possible State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>node1</td>
<td>-</td>
<td>Waiting for giveback (HA mailboxes)</td>
</tr>
<tr>
<td>node1</td>
<td>node0</td>
<td>false</td>
<td>In takeover</td>
</tr>
</tbody>
</table>
+------------------------------------------------------------------------------+
```

2 entries were displayed.

13. Wait at least eight minutes for the following conditions to take effect:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in an I/O operation that occurs during takeover.

The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

14. Return the aggregates to the first node:

storage failover giveback -ofnode nodenameA

The giveback first returns the root aggregate to the partner node and then, after that node has finished booting, returns the non-root aggregates and any LIFs that were set to automatically revert. The newly
booted node begins to serve data to clients from each aggregate as soon as the aggregate is returned.

15. Verify that all aggregates have been returned:

```
storage failover show-giveback
```

If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

16. If any aggregates have not been returned, perform the following steps:
   a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
   b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
   c. Rerun the storage failover giveback command.

   If you decided to override the “veto” condition, set the -override-vetoes parameter to true.

17. Wait at least eight minutes for the following conditions to take effect:
   - Client multipathing (if deployed) is stabilized.
   - Clients are recovered from the pause in an I/O operation that occurs during giveback.

   The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

18. Verify that the update was completed successfully for the node:
   a. Go to the advanced privilege level:

```
set -privilege advanced
```

   b. Verify that update status is complete for the node:

```
system node upgrade-revert show -node nodenameA
```

   The status should be listed as complete.

   If the status is not complete, contact technical support.

   c. Return to the admin privilege level:

```
set -privilege admin
```

19. Verify that the node’s ports are up:
network port show -node nodenameA

You must run this command on a node that is upgraded to the higher version of ONTAP 9.

The following example shows that all of the node’s ports are up:

```
cluster1::> network port show -node node0

Speed
(Mbps)
Node Port IPspace Broadcast Domain Link MTU Admin/Oper
------- --------- ------------ ---------------- ----- -------
node0 e0M Default - up 1500 auto/100
e0a Default - up 1500 auto/1000
e0b Default - up 1500 auto/1000
ea1a Cluster Cluster up 9000 auto/10000
ea1b Cluster Cluster up 9000 auto/10000

5 entries were displayed.
```

20. Revert the LIFs back to the node:

```
network interface revert *
```

This command returns the LIFs that were migrated away from the node.

```
cluster1::> network interface revert *
8 entries were acted on.
```

21. Verify that the node’s data LIFs successfully reverted back to the node, and that they are up:

```
network interface show
```

The following example shows that all of the data LIFs hosted by the node have successfully reverted back to the node, and that their operational status is up:
cluster1::> network interface show

Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
----------- ---------- ---------- ------------------ --------------
------- ----
Home
---------

vs0
data001   up/up    192.0.2.120/24     node0         e0a
data002   up/up    192.0.2.121/24     node0         e0b
true
true
data003   up/up    192.0.2.122/24     node0         e0b
true
data004   up/up    192.0.2.123/24     node0         e0a
true
4 entries were displayed.

22. If you previously determined that this node serves clients, verify that the node is providing service for each protocol that it was previously serving:

    system node run -node nodenameA -command uptime

The operation counts reset to zero during the update.

The following example shows that the updated node has resumed serving its NFS and iSCSI clients:

cluster1::> system node run -node node0 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP ops, 2 iSCSI ops

23. Reenable automatic giveback on the partner node if it was previously disabled:

    storage failover modify -node nodenameB -auto-giveback true

You should proceed to update the node’s HA partner as quickly as possible. If you must suspend the update process for any reason, both nodes in the HA pair should be running the same ONTAP version.

Updating the partner node in an HA pair

After updating the first node in an HA pair, you update its partner by initiating a takeover on it. The first node serves the partner’s data while the partner node is upgraded.
1. Set the privilege level to advanced, entering y when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (*>>) appears.

2. Set the new ONTAP software image to be the default image:

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

The system image modify command uses an extended query to change the new ONTAP software image (which is installed as the alternate image) to be the default image for the node.

3. Monitor the progress of the update:

```
system node upgrade-revert show
```

4. Verify that the new ONTAP software image is set as the default image:

```
system image show
```

In the following example, `image2` is the new version of ONTAP and is set as the default image on the node:

```
cluster1::*> system image show

<table>
<thead>
<tr>
<th>Node</th>
<th>Image</th>
<th>Default</th>
<th>Current</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>image1</td>
<td>false</td>
<td>false</td>
<td>X.X.X</td>
<td>MM/DD/YYYY TIME</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>true</td>
<td>Y.Y.Y</td>
<td>MM/DD/YYYY TIME</td>
</tr>
<tr>
<td>node1</td>
<td>image1</td>
<td>false</td>
<td>true</td>
<td>X.X.X</td>
<td>MM/DD/YYYY TIME</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>Y.Y.Y</td>
<td>MM/DD/YYYY TIME</td>
</tr>
</tbody>
</table>

4 entries were displayed.

5. Disable automatic giveback on the partner node if it is enabled:

```
storage failover modify -node nodenameA -auto-giveback false
```

If the cluster is a two-node cluster, a message is displayed warning you that disabling automatic giveback prevents the management cluster services from going online in the event of an alternating-failure scenario.
Enter y to continue.

6. Verify that automatic giveback is disabled for the partner node:

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node     auto-giveback
-------- --------------
node0    false
1 entry was displayed.
```

7. Run the following command twice to determine whether the node to be updated is currently serving any clients:

```
system node run -node nodenameB -command uptime
```

The uptime command displays the total number of operations that the node has performed for NFS, SMB, FC, and iSCSI clients since the node was last booted. For each protocol, you must run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

**NOTE:** You should make a note of each protocol that has increasing client operations so that after the node is updated, you can verify that client traffic has resumed.

The following example shows a node with NFS, SMB, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```
cluster1::> system node run -node node1 -command uptime
2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP ops, 40395 FCP ops, 32815 iSCSI ops
```

8. Migrate all of the data LIFs away from the node:

```
network interface migrate-all -node nodenameB
```

9. Verify the status of any LIFs that you migrated:
network interface show

For more information about parameters you can use to verify LIF status, see the network interface show man page.

The following example shows that node1’s data LIFs migrated successfully. For each LIF, the fields included in this example enable you to verify the LIF’s home node and port, the current node and port to which the LIF migrated, and the LIF’s operational and administrative status.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data -home-node node1 -fields home-node,curr-node,curr-port,home-port,status-admin,status-oper
vserver lif home-node home-port curr-node curr-port status-oper status-admin
----------- ------------ ------------- ------------- ------------- --------- --------------
vs0  data001 node1  e0a  node0  e0a  up           up
vs0  data002 node1  e0b  node0  e0b  up           up
vs0  data003 node1  e0b  node0  e0b  up           up
vs0  data004 node1  e0a  node0  e0a  up           up
4 entries were displayed.
```

10. Initiate a takeover:

```
storage failover takeover -ofnode nodenameB -option allow-version-mismatch
```

Do not specify the -option immediate parameter, because a normal takeover is required for the node that is being taken over to boot onto the new software image. If you did not manually migrate the LIFs away from the node, they automatically migrate to the node’s HA partner so that there are no service disruptions.

A warning is displayed. You must enter y to continue.

The node that is taken over boots up to the Waiting for giveback state.

If AutoSupport is enabled, an AutoSupport message is sent indicating that the node is out of cluster quorum. You can ignore this notification and proceed with the update.

11. Verify that the takeover was successful:

```
storage failover show
```

The following example shows that the takeover was successful. Node node1 is in the Waiting for giveback state, and its partner is in the In takeover state.
12. Wait at least eight minutes for the following conditions to take effect:
   +
      ◦ Client multipathing (if deployed) is stabilized.
      ◦ Clients are recovered from the pause in I/O that occurs during takeover.

The recovery time is client-specific and might take longer than eight minutes, depending on the characteristics of the client applications.

13. Return the aggregates to the partner node:

   ```
   storage failover giveback -ofnode nodenameB
   ```

   The giveback operation first returns the root aggregate to the partner node and then, after that node has finished booting, returns the non-root aggregates and any LIFs that were set to automatically revert. The newly booted node begins to serve data to clients from each aggregate as soon as the aggregate is returned.

14. Verify that all aggregates are returned:

   ```
   storage failover show-giveback
   ```

   If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates are returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback operation.

15. If any aggregates are not returned, perform the following steps:
   a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
   b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
   c. Rerun the storage failover giveback command.

      If you decided to override the “veto” condition, set the -override-vetoes parameter to true.

16. Wait at least eight minutes for the following conditions to take effect:
- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in an I/O operation that occurs during giveback.

The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

17. Verify that the update was completed successfully for the node:
   a. Go to the advanced privilege level:
      
      ```bash
      set -privilege advanced
      ```

   b. Verify that update status is complete for the node:
      
      ```bash
      system node upgrade-revert show -node nodenameB
      ```

      The status should be listed as complete.

      If the status is not complete, from the node, run the system node upgrade-revert upgrade command. If the command does not complete the update, contact technical support.

   c. Return to the admin privilege level:
      
      ```bash
      set -privilege admin
      ```

18. Verify that the node’s ports are up:

    ```bash
    network port show -node nodenameB
    ```

    You must run this command on a node that has been upgraded to ONTAP 9.4.

    The following example shows that all of the node's data ports are up:
19. Revert the LIFs back to the node:

```
cluster1::> network interface revert *
```

This command returns the LIFs that were migrated away from the node.

```
cluster1::> network interface revert *
8 entries were acted on.
```

20. Verify that the node’s data LIFs successfully reverted back to the node, and that they are up:

```
network interface show
```

The following example shows that all of the data LIFs hosted by the node is successfully reverted back to the node, and that their operational status is up:
cluster1::> network interface show

<table>
<thead>
<tr>
<th>Logical</th>
<th>Status</th>
<th>Network</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vserver</td>
<td>Interface</td>
<td>Admin/Oper</td>
<td>Address/Mask</td>
</tr>
<tr>
<td>Home</td>
<td>-----------</td>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td>---------</td>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>vs0</td>
<td>data001</td>
<td>up/up</td>
<td>192.0.2.120/24</td>
</tr>
<tr>
<td>true</td>
<td>data002</td>
<td>up/up</td>
<td>192.0.2.121/24</td>
</tr>
<tr>
<td>true</td>
<td>data003</td>
<td>up/up</td>
<td>192.0.2.122/24</td>
</tr>
<tr>
<td>true</td>
<td>data004</td>
<td>up/up</td>
<td>192.0.2.123/24</td>
</tr>
</tbody>
</table>

4 entries were displayed.

21. If you previously determined that this node serves clients, verify that the node is providing service for each protocol that it was previously serving:

```
system node run -node nodenameB -command uptime
```

The operation counts reset to zero during the update.

The following example shows that the updated node has resumed serving its NFS and iSCSI clients:

```
cluster1::> system node run -node node1 -command uptime
            3:15pm up 0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP ops, 2 iSCSI ops
```

22. If this was the last node in the cluster to be updated, trigger an AutoSupport notification:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

This AutoSupport notification includes a record of the system status just prior to update. It saves useful troubleshooting information in case there is a problem with the update process.

If the cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

23. Confirm that the new ONTAP software is running on both nodes of the HA pair:
set -privilege advanced

system node image show

In the following example, image2 is the updated version of ONTAP and is the default version on both nodes:

```
cluster1::*> system node image show
       Is  Is                Install
       ---- ------- ------- ------- --------- -------------------
       Node Image Default Current Version    Date
       -------- ------- ------- ------- --------- -------------------
       node0
       image1 false false   X.X.X     MM/DD/YYYY TIME
       image2 true  true    Y.Y.Y     MM/DD/YYYY TIME
       node1
       image1 false false   X.X.X     MM/DD/YYYY TIME
       image2 true  true    Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

24. Reenable automatic giveback on the partner node if it was previously disabled:

```
storage failover modify -node nodenameA -auto-giveback true
```

25. Verify that the cluster is in quorum and that services are running by using the `cluster show` and `cluster ring show` (advanced privilege level) commands.

You must perform this step before upgrading any additional HA pairs.

26. Return to the admin privilege level:

```
set -privilege admin
```

27. Upgrade any additional HA pairs.

**Manual nondisruptive ONTAP upgrade of a four- or eight-node MetroCluster configuration using the CLI**

A manual upgrade of a four- or eight-node MetroCluster configuration involves preparing for the update, updating the DR pairs in each of the one or two DR groups simultaneously, and performing post-upgrade tasks.

- This task applies to the following configurations:
  - Four-node MetroCluster FC or IP configurations running ONTAP 9.2 or earlier
- Eight-node MetroCluster FC configurations, regardless of ONTAP version
- If you have a two-node MetroCluster configuration, do not use this procedure.
- The following tasks refer to the old and new versions of ONTAP.
  - When upgrading, the old version is a previous version of ONTAP, with a lower version number than the new version of ONTAP.
  - When downgrading, the old version is a later version of ONTAP, with a higher version number than the new version of ONTAP.
- This task uses the following high-level workflow:
Differences when updating ONTAP software on an eight-node or four-node MetroCluster configuration

The MetroCluster software upgrade process differs, depending on whether there are eight or four nodes in the MetroCluster configuration.

A MetroCluster configuration consists of one or two DR groups. Each DR group consists of two HA pairs, one HA pair at each MetroCluster cluster. An eight-node MetroCluster includes two DR groups:

For four-node MetroCluster configurations:
1. Upgrade DR Group One:
   a. Upgrade node_A_1 and node_B_1.
   b. Upgrade node_A_2 and node_B_2.

For eight-node MetroCluster configurations, you perform the DR group upgrade procedure twice:
1. Upgrade DR Group One:
   a. Upgrade node_A_1 and node_B_1.
   b. Upgrade node_A_2 and node_B_2.
2. Upgrade DR Group Two:
   a. Upgrade node_A_3 and node_B_3.
   b. Upgrade node_A_4 and node_B_4.
Preparing to upgrade a MetroCluster DR group

Before you upgrade the ONTAP software on the nodes, you must identify the DR relationships among the nodes, send an AutoSupport message that you are initiating an upgrade, and confirm the ONTAP version running on each node.

You must have downloaded and installed the software images.

This task must be repeated on each DR group. If the MetroCluster configuration consists of eight nodes, there are two DR groups. Thereby, this task must be repeated on each DR group.

The examples provided in this task use the names shown in the following illustration to identify the clusters and nodes:

1. Identify the DR pairs in the configuration:

   `metrocluster node show -fields dr-partner`
2. Set the privilege level from admin to advanced, entering y when prompted to continue:

   set -privilege advanced

   The advanced prompt (*>>) appears.

3. Confirm the ONTAP version on cluster_A:

   system image show

   cluster_A::*> system image show

   Is      Is                Install
   Node     Image   Default Current Version   Date
   -------- ------- ------- ------- -------   -------------------
   node_A_1 image1  true    true    X.X.X     MM/DD/YYYY TIME
   image2  false   false   Y.Y.Y     MM/DD/YYYY TIME
   node_A_2 image1  true    true    X.X.X     MM/DD/YYYY TIME
   image2  false   false   Y.Y.Y     MM/DD/YYYY TIME

   4 entries were displayed.

   cluster_A::>

4. Confirm the version on cluster_B:

   system image show
cluster_B::*> system image show

<table>
<thead>
<tr>
<th>Node</th>
<th>Image</th>
<th>Default</th>
<th>Current Version</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_B_1</td>
<td>image1</td>
<td>true</td>
<td>true</td>
<td>X.X.X</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>false</td>
<td>false</td>
<td>Y.Y.Y</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>node_B_2</td>
<td>image1</td>
<td>true</td>
<td>true</td>
<td>X.X.X</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>false</td>
<td>false</td>
<td>Y.Y.Y</td>
<td>MM/DD/YYYY</td>
</tr>
</tbody>
</table>

4 entries were displayed.

5. Trigger an AutoSupport notification:

   autosupport invoke -node * -type all -message "Starting_NDU"

This AutoSupport notification includes a record of the system status before the upgrade. It saves useful troubleshooting information if there is a problem with the upgrade process.

If your cluster is not configured to send AutoSupport messages, then a copy of the notification is saved locally.

6. For each node in the first set, set the target ONTAP software image to be the default image:

   system image modify {-node nodename -iscurrent false} -isdefault true

This command uses an extended query to change the target software image, which is installed as the alternate image, to be the default image for the node.

7. Verify that the target ONTAP software image is set as the default image on cluster_A:

   system image show

   In the following example, image2 is the new ONTAP version and is set as the default image on each of the nodes in the first set:
a. Verify that the target ONTAP software image is set as the default image on cluster_B:

```
  system image show
```

The following example shows that the target version is set as the default image on each of the nodes in the first set:

```
cluster_B::*> system image show
  Is     Is              Install
 Node   Image  Default Current Version Date
       ------ ------- ------- ------- ------- -------------------
node_A_1  image1 false  true   X.X.X   MM/DD/YYYY TIME
          image2 true  false   Y.Y.Y   MM/DD/YYYY TIME
node_A_2  image1 false  true   X.X.X   MM/DD/YYYY TIME
          image2 true  false   Y.Y.Y   MM/DD/YYYY TIME
2 entries were displayed.
```

8. Determine whether the nodes to be upgraded are currently serving any clients twice for each node:

```
system node run -node target-node -command uptime
```

The uptime command displays the total number of operations that the node has performed for NFS, CIFS, FC, and iSCSI clients since the node was last booted. For each protocol, you need to run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.
You should make a note of each protocol that has increasing client operations so that after the node is upgraded, you can verify that client traffic has resumed.

This example shows a node with NFS, CIFS, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```
cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP ops, 40395 FCP ops, 32810 iSCSI ops

cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP ops, 40395 FCP ops, 32815 iSCSI ops
```

**Updating the first DR pair in a MetroCluster DR group**

You must perform a takeover and giveback of the nodes in the correct order to make the new version of ONTAP the current version of the node.

All nodes must be running the old version of ONTAP.

In this task, node_A_1 and node_B_1 are upgraded.

If you have upgraded the ONTAP software on the first DR group, and are now upgrading the second DR group in an eight-node MetroCluster configuration, in this task you would be updating node_A_3 and node_B_3.

1. If MetroCluster Tiebreaker software is enabled, disabled it.
2. For each node in the HA pair, disable automatic giveback:

   ```
   storage failover modify -node target-node -auto-giveback false
   ```

   This command must be repeated for each node in the HA pair.

3. Verify that automatic giveback is disabled:

   ```
   storage failover show -fields auto-giveback
   ```

   This example shows that automatic giveback has been disabled on both nodes:
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
--------- --------------
node_x_1 false
node_x_2 false
2 entries were displayed.

4. Ensure that I/O is not exceeding ~50% for each controller and that CPU utilization is not exceeding ~50% per controller.

5. Initiate a takeover of the target node on cluster_A:

   Do not specify the -option immediate parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

   a. Take over the DR partner on cluster_A (node_A_1):

   
   ```
   storage failover takeover -ofnode node_A_1
   ```

   The node boots up to the "Waiting for giveback" state.

   If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

   b. Verify that the takeover is successful:

   ```
   storage failover show
   ```

   The following example shows that the takeover is successful. Node_A_1 is in the "Waiting for giveback" state and node_A_2 is in the "In takeover" state.

   ```
   cluster1::> storage failover show
   Takeover
   Node     Partner          Possible State Description
   -------------- -------------- --------
   node_A_1      node_A_2      -       Waiting for giveback (HA mailboxes)
   node_A_2      node_A_1      false    In takeover
   2 entries were displayed.
   ```

6. Take over the DR partner on cluster_B (node_B_1):

   Do not specify the -option immediate parameter, because a normal takeover is required for the nodes that...
are being taken over to boot onto the new software image.

a. Take over node_B_1:

```bash
storage failover takeover -ofnode node_B_1
```

The node boots up to the "Waiting for giveback" state.

If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

b. Verify that the takeover is successful:

```bash
storage failover show
```

The following example shows that the takeover is successful. Node_B_1 is in the "Waiting for giveback" state and node_B_2 is in the "In takeover" state.

```
cluster1::> storage failover show
Takeover
Node Partner Possible State Description
-------------- -------------- --------
-------------------------------------
node_B_1 node_B_2 -        Waiting for giveback (HA mailboxes)
node_B_2 node_B_1 false    In takeover
2 entries were displayed.
```

7. Wait at least eight minutes to ensure the following conditions:
   - Client multipathing (if deployed) is stabilized.
   - Clients are recovered from the pause in I/O that occurs during takeover.

   The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

8. Return the aggregates to the target nodes:

   After upgrading MetroCluster IP configurations to ONTAP 9.5 or later, the aggregates will be in a degraded state for a short period before resynchronizing and returning to a mirrored state.

   a. Give back the aggregates to the DR partner on cluster_A:

   ```bash
   storage failover giveback -ofnode node_A_1
   ```
b. Give back the aggregates to the DR partner on cluster_B:

```
storage failover giveback -ofnode node_B_1
```

The giveback operation first returns the root aggregate to the node and then, after the node has finished booting, returns the non-root aggregates.

9. Verify that all aggregates have been returned by issuing the following command on both clusters:

```
storage failover show-giveback
```

If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

10. If any aggregates have not been returned, do the following:
    a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
    b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
    c. Reenter the storage failover giveback command.

        If you decided to override the “veto” condition, set the -override-vetoes parameter to true.

11. Wait at least eight minutes to ensure the following conditions:
    - Client multipathing (if deployed) is stabilized.
    - Clients are recovered from the pause in I/O that occurs during giveback.

        The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

12. Set the privilege level from admin to advanced, entering y when prompted to continue:

```
set -privilege advanced
```

        The advanced prompt (*>>) appears.

13. Confirm the version on cluster_A:

```
system image show
```

        The following example shows that System image2 should is the default and current version on node_A_1:
cluster_A::*> system image show

<table>
<thead>
<tr>
<th>Node</th>
<th>Image</th>
<th>Default</th>
<th>Current</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_A_1</td>
<td>image1</td>
<td>false</td>
<td>false</td>
<td>X.X.X</td>
<td>MM/DD/YYYY TIME</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>true</td>
<td>Y.Y.Y</td>
<td>MM/DD/YYYY TIME</td>
</tr>
<tr>
<td>node_A_2</td>
<td>image1</td>
<td>false</td>
<td>true</td>
<td>X.X.X</td>
<td>MM/DD/YYYY TIME</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>Y.Y.Y</td>
<td>MM/DD/YYYY TIME</td>
</tr>
</tbody>
</table>

4 entries were displayed.

14. Confirm the version on cluster_B:

system image show

The following example shows that System image2 (ONTAP 9.0.0) is the default and current version on node_A_1:

cluster_A::*> system image show

<table>
<thead>
<tr>
<th>Node</th>
<th>Image</th>
<th>Default</th>
<th>Current</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_B_1</td>
<td>image1</td>
<td>false</td>
<td>false</td>
<td>X.X.X</td>
<td>MM/DD/YYYY TIME</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>true</td>
<td>Y.Y.Y</td>
<td>MM/DD/YYYY TIME</td>
</tr>
<tr>
<td>node_B_2</td>
<td>image1</td>
<td>false</td>
<td>true</td>
<td>X.X.X</td>
<td>MM/DD/YYYY TIME</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>Y.Y.Y</td>
<td>MM/DD/YYYY TIME</td>
</tr>
</tbody>
</table>

4 entries were displayed.

cluster_A::>

**Updating the second DR pair in a MetroCluster DR group**

You must perform a takeover and giveback of the node in the correct order to make the new version of ONTAP the current version of the node.

You should have upgraded the first DR pair (node_A_1 and node_B_1).

In this task, node_A_2 and node_B_2 are upgraded.

If you have upgraded the ONTAP software on the first DR group, and are now updating the second DR group
in an eight-node MetroCluster configuration, in this task you are updating node_A_4 and node_B_4.

1. Migrate all of the data LIFs away from the node:

```
network interface migrate-all -node nodenameA
```

2. Initiate a takeover of the target node on cluster_A:

Do not specify the -option immediate parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

   a. Take over the DR partner on cluster_A:

```
storage failover takeover -ofnode node_A_2 -option allow-version-mismatch
```

   The allow-version-mismatch option is not required for upgrades from ONTAP 9.0 to ONTAP 9.1 or for any patch upgrades.

   The node boots up to the "Waiting for giveback" state.

   If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

   b. Verify that the takeover is successful:

```
storage failover show
```

   The following example shows that the takeover is successful. Node_A_2 is in the "Waiting for giveback" state and node_A_1 is in the "In takeover" state.

```
cluster1::> storage failover show

<table>
<thead>
<tr>
<th>Node</th>
<th>Partner</th>
<th>Possible State Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_A_1</td>
<td>node_A_2</td>
<td>false In takeover</td>
</tr>
<tr>
<td>node_A_2</td>
<td>node_A_1</td>
<td>- Waiting for giveback (HA mailboxes)</td>
</tr>
</tbody>
</table>

2 entries were displayed.

3. Initiate a takeover of the target node on cluster_B:

Do not specify the -option immediate parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.
a. Take over the DR partner on cluster_B (node_B_2):

<table>
<thead>
<tr>
<th>If you are upgrading from...</th>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP 9.2 or ONTAP 9.1</td>
<td><code>storage failover takeover -ofnode node_B_2</code></td>
</tr>
<tr>
<td>ONTAP 9.0 or Data ONTAP 8.3.x</td>
<td><code>storage failover takeover -ofnode node_B_2 -option allow-version-mismatch</code></td>
</tr>
</tbody>
</table>

The node boots up to the "Waiting for giveback" state.

If AutoSupport is enabled, an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can safely ignore this notification and proceed with the upgrade.

b. Verify that the takeover is successful:

`storage failover show`

The following example shows that the takeover is successful. Node_B_2 is in the "Waiting for giveback" state and node_B_1 is in the "In takeover" state.

```
cluster1:~ > storage failover show
Takeover
Node          Partner          Possible State Description
-------------- -------------- --------
node_B_1       node_B_2       false    In takeover
node_B_2       node_B_1       -        Waiting for giveback (HA mailboxes)
2 entries were displayed.
```

4. Wait at least eight minutes to ensure the following conditions:
   - Client multipathing (if deployed) is stabilized.
   - Clients are recovered from the pause in I/O that occurs during takeover.

The `allow-version-mismatch` option is not required for upgrades from ONTAP 9.0 to ONTAP 9.1 or for any patch upgrades.
The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

5. Return the aggregates to the target nodes:

After upgrading MetroCluster IP configurations to ONTAP 9.5, the aggregates will be in a degraded state for a short period before resynchronizing and returning to a mirrored state.

   a. Give back the aggregates to the DR partner on cluster_A:

   ```
   storage failover giveback -ofnode node_A_2
   ```

   b. Give back the aggregates to the DR partner on cluster_B:

   ```
   storage failover giveback -ofnode node_B_2
   ```

   The giveback operation first returns the root aggregate to the node and then, after the node has finished booting, returns the non-root aggregates.

6. Verify that all aggregates have been returned by issuing the following command on both clusters:

   ```
   storage failover show-giveback
   ```

   If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

7. If any aggregates have not been returned, do the following:

   a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.

   b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.

   c. Reenter the storage failover giveback command.

      If you decided to override the “veto” condition, set the -override-vetoes parameter to true.

8. Wait at least eight minutes to ensure the following conditions:

   - Client multipathing (if deployed) is stabilized.
   - Clients are recovered from the pause in I/O that occurs during giveback.

   The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

9. Set the privilege level from admin to advanced, entering y when prompted to continue:

   ```
   set -privilege advanced
   ```
The advanced prompt (*>>) appears.

10. Confirm the version on cluster_A:

```
system image show
```

The following example shows that System image2 (target ONTAP image) is the default and current version on node_A_2:

```
cluster_B::*> system image show
<table>
<thead>
<tr>
<th>Is</th>
<th>Is</th>
<th>Install</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Image</td>
<td>Default</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>node_A_1</td>
<td>image1</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
</tr>
<tr>
<td>node_A_2</td>
<td>image1</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
</tr>
</tbody>
</table>
```

4 entries were displayed.

cluster_A::>

11. Confirm the version on cluster_B:

```
system image show
```

The following example shows that System image2 (target ONTAP image) is the default and current version on node_B_2:

```
cluster_B::*> system image show
<table>
<thead>
<tr>
<th>Is</th>
<th>Is</th>
<th>Install</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Image</td>
<td>Default</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>node_B_1</td>
<td>image1</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
</tr>
<tr>
<td>node_B_2</td>
<td>image1</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
</tr>
</tbody>
</table>
```

4 entries were displayed.

cluster_A::>
12. For each node in the HA pair, enable automatic giveback:

```
storage failover modify -node target-node -auto-giveback true
```

This command must be repeated for each node in the HA pair.

13. Verify that automatic giveback is enabled:

```
storage failover show -fields auto-giveback
```

This example shows that automatic giveback has been enabled on both nodes:

```
cluster_x:/> storage failover show -fields auto-giveback
node     auto-giveback
-------- --------------
node_x_1 true
node_x_2 true
2 entries were displayed.
```

**Nondisruptive upgrade of a two-node MetroCluster configuration in ONTAP 9.2 or earlier**

How you upgrade a two-node MetroCluster configuration varies based on your ONTAP version. If you are running ONTAP 9.2 or earlier, you should use this procedure to perform a manual nondisruptive upgrade which includes initiating a negotiated switchover, updating the cluster at the “failed” site, initiating switchback, and then repeating the process on the cluster at the other site.

If you have a two-node MetroCluster configuration running ONTAP 9.3 or later, perform an automated upgrade using System Manager.

**Steps**

1. Set the privilege level to advanced, entering y when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (>*>) appears.

2. On the cluster to be upgraded, install the new ONTAP software image as the default:

```
system node image update -package package_location -setdefault true -replace-package true
```
cluster_B::*> system node image update -package http://www.example.com/NewImage.tgz -setdefault true -replace-package true

3. Verify that the target software image is set as the default image:

    system node image show

The following example shows that NewImage is set as the default image:

    cluster_B::*> system node image show

<table>
<thead>
<tr>
<th>Node</th>
<th>Image</th>
<th>Default</th>
<th>Current Version</th>
<th>Install</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_B_1</td>
<td>OldImage</td>
<td>false</td>
<td>true</td>
<td>X.X.X MM/DD/YYYY</td>
</tr>
<tr>
<td></td>
<td>NewImage</td>
<td>true</td>
<td>false</td>
<td>Y.Y.Y MM/DD/YYYY</td>
</tr>
</tbody>
</table>

    2 entries were displayed.

4. If the target software image is not set as the default image, then change it:

    system image modify {-node * -iscurrent false} -isdefault true

5. Verify that all cluster SVMs are in a health state:

    metrocluster vserver show

6. On the cluster that is not being updated, initiate a negotiated switchover:

    metrocluster switchover

The operation can take several minutes. You can use the metrocluster operation show command to verify that the switchover is completed.

In the following example, a negotiated switchover is performed on the remote cluster ("cluster_A"). This causes the local cluster ("cluster_B") to halt so that you can update it.
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data

  Vservers on cluster "cluster_B" and
  automatically re-start them on cluster
  "cluster_A". It will finally gracefully shutdown
  cluster "cluster_B".
Do you want to continue? {y|n}: y

7. Verify that all cluster SVMs are in a health state:

   metrocluster vserver show

8. Resynchronize the data aggregates on the “surviving” cluster:

   metrocluster heal -phase aggregates

After upgrading MetroCluster IP configurations to ONTAP 9.5 or later, the aggregates will be in a degraded
state for a short period before resynchronizing and returning to a mirrored state.

   cluster_A::> metrocluster heal -phase aggregates
   [Job 130] Job succeeded: Heal Aggregates is successful.

9. Verify that the healing operation was completed successfully:

   metrocluster operation show

   cluster_A::> metrocluster operation show
   Operation: heal-aggregates
   State: successful
   Start Time: MM/DD/YYYY TIME
   End Time: MM/DD/YYYY TIME
   Errors: -

10. Resynchronize the root aggregates on the “surviving” cluster:

    metrocluster heal -phase root-aggregates
11. Verify that the healing operation was completed successfully:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. On the halted cluster, boot the node from the LOADER prompt:

```
boot_ontap
```

13. Wait for the boot process to finish, and then verify that all cluster SVMs are in a health state:

```
metrocluster vserver show
```

14. Perform a switchback from the “surviving” cluster:

```
metrocluster switchback
```

15. Verify that the switchback was completed successfully:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. Verify that all cluster SVMs are in a health state:
metrocluster vserver show

17. Repeat all previous steps on the other cluster.
18. Verify that the MetroCluster configuration is healthy:
   a. Check the configuration:

metrocluster check run

cluster_A::> metrocluster check run
Last Checked On: MM/DD/YYYY TIME
Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

b. If you want to view more detailed results, use the metrocluster check run command:

metrocluster check aggregate show

metrocluster check config-replication show

metrocluster check lif show

metrocluster check node show

c. Set the privilege level to advanced:
d. Simulate the switchover operation:

```
set -privilege advanced
```

```
metrocluster switchover -simulate
```

e. Review the results of the switchover simulation:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
Operation: switchover
    State: successful
    Start time: MM/DD/YYYY TIME
    End time: MM/DD/YYYY TIME
    Errors: -
```

f. Return to the admin privilege level:

```
set -privilege admin
```

g. Repeat these substeps on the other cluster.

After you finish

Perform any post-upgrade tasks.

Related information

MetroCluster Disaster recovery

Manual disruptive ONTAP upgrade using the CLI

If you can take your cluster offline to upgrade to a new ONTAP release, then you can use the disruptive upgrade method. This method has several steps: disabling storage failover for each HA pair, rebooting each node in the cluster, and then reenabling storage failover.

- You must download and install the software image.
- If you are operating in a SAN environment, all SAN clients must be shut down or suspended until the upgrade is complete.

If SAN clients are not shut down or suspended prior to a disruptive upgrade, then the client file systems and applications suffer errors that might require manual recovery after the upgrade is completed.

In a disruptive upgrade, downtime is required because storage failover is disabled for each HA pair, and each
node is updated. When storage failover is disabled, each node behaves as a single-node cluster; that is, system services associated with the node are interrupted for as long as it takes the system to reboot.

Steps
1. Set the privilege level from admin to advanced, entering y when prompted to continue:

   ```
   set -privilege advanced
   ```

   The advanced prompt (*>>) appears.

2. Set the new ONTAP software image to be the default image:

   ```
   system image modify {-node * -iscurrent false} -isdefault true
   ```

   This command uses an extended query to change the target ONTAP software image (which is installed as the alternate image) to be the default image for each node.

3. Verify that the new ONTAP software image is set as the default image:

   ```
   system image show
   ```

   In the following example, image 2 is the new ONTAP version and is set as the default image on both nodes:

<table>
<thead>
<tr>
<th>Node</th>
<th>Image</th>
<th>Default</th>
<th>Current Version</th>
<th>Install</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>image1</td>
<td>false</td>
<td>true</td>
<td>X.X.X</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>Y.Y.Y</td>
</tr>
<tr>
<td>node1</td>
<td>image1</td>
<td>false</td>
<td>true</td>
<td>X.X.X</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>Y.Y.Y</td>
</tr>
</tbody>
</table>

   4 entries were displayed.

4. Perform either one of the following steps:

<table>
<thead>
<tr>
<th>If the cluster consists of...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>One node</td>
<td>Continue to the next step.</td>
</tr>
<tr>
<td>If the cluster consists of…</td>
<td>Do this…</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Two nodes</td>
<td>a. Disable cluster high availability:</td>
</tr>
<tr>
<td></td>
<td><code>cluster ha modify -configured false</code></td>
</tr>
<tr>
<td></td>
<td><strong>Enter y to continue when prompted.</strong></td>
</tr>
<tr>
<td></td>
<td>b. Disable storage failover for the HA pair:</td>
</tr>
<tr>
<td></td>
<td><code>storage failover modify -node * -enabled false</code></td>
</tr>
<tr>
<td>More than two nodes</td>
<td>Disable storage failover for each HA pair in the cluster:</td>
</tr>
<tr>
<td></td>
<td><code>storage failover modify -node * -enabled false</code></td>
</tr>
</tbody>
</table>

5. Reboot a node in the cluster:

```
system node reboot -node nodename -ignore-quorum-warnings
```

> **i** Do not reboot more than one node at a time.

The node boots the new ONTAP image. The ONTAP login prompt appears, indicating that the reboot process is complete.

6. After the node or set of nodes has rebooted with the new ONTAP image, set the privilege level to advanced:

```
set -privilege advanced
```

**Enter y when prompted to continue**

7. Confirm that the new software is running:

```
system node image show
```

In the following example, image1 is the new ONTAP version and is set as the current version on node0:
8. Verify that the upgrade is completed successfully:
   a. Set the privilege level to advanced:

   ```bash
   set -privilege advanced
   ```

   b. Verify that the upgrade status is complete for each node:

   ```bash
   system node upgrade-revert show -node nodename
   ```

   The status should be listed as complete.

   If the status is not complete, contact NetApp Support immediately.

   c. Return to the admin privilege level:

   ```bash
   set -privilege admin
   ```

9. Repeat Steps 2 through 8 for each additional node.

10. If the cluster consists of two or more nodes, enable storage failover for each HA pair in the cluster:

    ```bash
    storage failover modify -node * -enabled true
    ```

11. If the cluster consists of only two nodes, enable cluster high availability:

    ```bash
    cluster ha modify -configured true
    ```
What to do after an ONTAP upgrade

After you upgrade ONTAP, there are several tasks you should perform to verify your cluster readiness.

1. Verify your cluster.

After you upgrade ONTAP, you should verify your cluster version, cluster health, and storage health. If you are using a MetroCluster FC configuration, you also need to verify that the cluster is enabled for automatic unplanned switchover.

2. Verify that all LIFs are on home ports.

During a reboot, some LIFs might have been migrated to their assigned failover ports. After you upgrade a cluster, you must enable and revert any LIFs that are not on their home ports.

3. Verify special considerations specific to your cluster.

If certain configurations exist on your cluster, you might need to perform additional steps after you upgrade.


The DQP is not updated as part of an ONTAP upgrade.

Verify your cluster after ONTAP upgrade

After you upgrade ONTAP, verify the cluster version, cluster health, and storage health. For MetroCluster FC configurations, also verify that the cluster is enabled for automatic unplanned switchover.

**Verify cluster version**

After all the HA pairs have been upgraded, you must use the version command to verify that all of the nodes are running the target release.

The cluster version is the lowest version of ONTAP running on any node in the cluster. If the cluster version is not the target ONTAP release, you can upgrade your cluster.

1. Verify that the cluster version is the target ONTAP release:

   ```
   version
   ```

2. If the cluster version is not the target ONTAP release, you should verify the upgrade status of all nodes:

   ```
   system node upgrade-revert show
   ```
Verify cluster health

After you upgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster:

   ```
   cluster show
   ```

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node0                 true    true
   node1                 true    true
   ```

   If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

3. Verify the configuration details for each RDB process.

   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.

   Note that each ring might have a different quorum master.

<table>
<thead>
<tr>
<th>To display this RDB process...</th>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management application</td>
<td>cluster ring show -unitname mgmt</td>
</tr>
<tr>
<td>Volume location database</td>
<td>cluster ring show -unitname vldb</td>
</tr>
<tr>
<td>Virtual-Interface manager</td>
<td>cluster ring show -unitname vifmgr</td>
</tr>
<tr>
<td>SAN management daemon</td>
<td>cluster ring show -unitname bcomd</td>
</tr>
</tbody>
</table>

   This example shows the volume location database process:
4. If you are operating in a SAN environment, verify that each node is in a SAN quorum:

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
Master        Cluster        Quorum     Availability
Operational   Node          Status      Status      Status
----------------- ----------------- ------------- ------------- -------------
cluster1-01     cluster1-01   in-quorum    true
operational     cluster1-02   in-quorum    true
operational     
2 entries were displayed.
```

**Related information**

**System administration**

**Verify automatic unplanned switchover is enabled (MetroCluster FC configurations only)**

If your cluster is in a MetroCluster FC configuration, you should verify that automatic unplanned switchover is enabled after you upgrade ONTAP.

If you are using a MetroCluster IP configuration, skip this procedure.

**Steps**

1. Check whether automatic unplanned switchover is enabled:

```
metrocluster show
```

If automatic unplanned switchover is enabled, the following statement appears in the command output:
AUSO Failure Domain auso-on-cluster-disaster

2. If the statement does not appear, enable an automatic unplanned switchover:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster
```

3. Verify that an automatic unplanned switchover has been enabled:

```
metrocluster show
```

Related information

Disk and aggregate management

Verify all LIFS are on home ports after ONTAP upgrade

During the reboot that occurs as part of the ONTAP upgrade process, some LIFs might be migrated from their home ports to their assigned failover ports. After an upgrade, you need to enable and revert any LIFs that are not on their home ports.

Steps

1. Display the status of all LIFs:

```
network interface show -fields home-port,curr-port
```

If Status Admin is "down" or Is home is "false" for any LIFs, continue with the next step.

2. Enable the data LIFs:

```
network interface modify {-role data} -status-admin up
```

3. Revert LIFs to their home ports:

```
network interface revert *
```

4. Verify that all LIFs are in their home ports:

```
network interface show
```

This example shows that all LIFs for SVM vs0 are on their home ports.
cluster1::> network interface show -vserver vs0

<table>
<thead>
<tr>
<th>Logical Status</th>
<th>Network Address/Mask</th>
<th>Current Port</th>
<th>Current Is</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vserver Interface</td>
<td>Admin/Oper Node</td>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>--------</td>
<td>-----</td>
</tr>
<tr>
<td>vs0 data001</td>
<td>up/up</td>
<td>192.0.2.120/24</td>
<td>node0</td>
</tr>
<tr>
<td>data002</td>
<td>up/up</td>
<td>192.0.2.121/24</td>
<td>node0</td>
</tr>
<tr>
<td>data003</td>
<td>up/up</td>
<td>192.0.2.122/24</td>
<td>node0</td>
</tr>
<tr>
<td>data004</td>
<td>up/up</td>
<td>192.0.2.123/24</td>
<td>node0</td>
</tr>
<tr>
<td>data005</td>
<td>up/up</td>
<td>192.0.2.124/24</td>
<td>node1</td>
</tr>
<tr>
<td>data006</td>
<td>up/up</td>
<td>192.0.2.125/24</td>
<td>node1</td>
</tr>
<tr>
<td>data007</td>
<td>up/up</td>
<td>192.0.2.126/24</td>
<td>node1</td>
</tr>
<tr>
<td>data008</td>
<td>up/up</td>
<td>192.0.2.127/24</td>
<td>node1</td>
</tr>
</tbody>
</table>

8 entries were displayed.

Special configurations

Special considerations after an ONTAP upgrade

If your cluster is configured with any of the following features you might need to perform additional steps after you upgrade your ONTAP software.

<table>
<thead>
<tr>
<th>Ask yourself…</th>
<th>If your answer is yes, then do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did I upgrade from ONTAP 9.7 or earlier to ONTAP 9.8 or later?</td>
<td>Verify your network configuration</td>
</tr>
<tr>
<td></td>
<td>Remove the EMS LIF service from network service polices that do not provide reachability to the EMS destination</td>
</tr>
<tr>
<td>Is my cluster in a a MetroCluster configuration?</td>
<td>Verify your networking and storage status</td>
</tr>
<tr>
<td>Do I have a SAN configuration?</td>
<td>Verify your SAN configuration</td>
</tr>
<tr>
<td>Did I upgrade from ONTAP 9.3 or earlier, and am using NetApp Storage Encryption?</td>
<td>Reconfigure KMIP server connections</td>
</tr>
<tr>
<td>Do I have load-sharing mirrors?</td>
<td>Relocate moved load-sharing mirror source volumes</td>
</tr>
<tr>
<td>Does my cluster have defined SnapMirror relationships?</td>
<td>Resume SnapMirror operations</td>
</tr>
<tr>
<td>Do I have user accounts for Service Processor (SP) access that were created prior to ONTAP 9.9.1?</td>
<td>Verify the change in accounts that can access the Service Processor</td>
</tr>
</tbody>
</table>

Verify your networking configuration after an ONTAP upgrade from ONTAP 9.7x or earlier

After you upgrade from ONTAP 9.7x or earlier to ONTAP 9.8 or later, you should verify your network configuration. After the upgrade, ONTAP automatically monitors layer 2 reachability.
Step

1. Verify each port has reachability to its expected broadcast domain:

   network port reachability show -detail

The command output contains reachability results. Use the following decision tree and table to understand the reachability results (reachability-status) and determine what, if anything, to do next.
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ok</strong></td>
<td>The port has layer 2 reachability to its assigned broadcast domain.</td>
</tr>
<tr>
<td></td>
<td>If the reachability-status is &quot;ok&quot;, but there are &quot;unexpected ports&quot;, consider merging one or more broadcast domains. For more information, see Merge broadcast domains.</td>
</tr>
<tr>
<td></td>
<td>If the reachability-status is &quot;ok&quot;, but there are &quot;unreachable ports&quot;, consider splitting one or more broadcast domains. For more information, see Split broadcast domains.</td>
</tr>
<tr>
<td></td>
<td>If the reachability-status is &quot;ok&quot;, and there are no unexpected or unreachable ports, your configuration is correct.</td>
</tr>
<tr>
<td><strong>misconfigured-reachability</strong></td>
<td>The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain.</td>
</tr>
<tr>
<td></td>
<td>You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability:</td>
</tr>
<tr>
<td></td>
<td><code>network port reachability repair -node -port</code></td>
</tr>
<tr>
<td></td>
<td>For more information, see Repair port reachability.</td>
</tr>
<tr>
<td><strong>no-reachability</strong></td>
<td>The port does not have layer 2 reachability to any existing broadcast domain.</td>
</tr>
<tr>
<td></td>
<td>You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace:</td>
</tr>
<tr>
<td></td>
<td><code>network port reachability repair -node -port</code></td>
</tr>
<tr>
<td></td>
<td>For more information, see Repair port reachability.</td>
</tr>
<tr>
<td><strong>multi-domain-reachability</strong></td>
<td>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</td>
</tr>
<tr>
<td></td>
<td>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port’s assigned broadcast domain needs to be merged with one or more broadcast domains.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Merge broadcast domains or Repair port reachability.</td>
</tr>
<tr>
<td><strong>unknown</strong></td>
<td>If the reachability-status is &quot;unknown&quot;, then wait a few minutes and try the command again.</td>
</tr>
</tbody>
</table>

After you repair a port, you need to check for and resolve displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group. For more information, see Repair port reachability.

**Remove EMS LIF service from network service policies**

If you have Event Management System (EMS) messages set up before you upgrade from ONTAP 9.7 or earlier to ONTAP 9.8 or later, after the upgrade, your EMS messages
might not be delivered.

During the upgrade, management-ems, which is the EMS LIF service, is added to all existing service polices. This allows EMS messages to be sent from any of the LIFs associated with any of the service polices. If the selected LIF does not have reachability to the event notification destination, the message is not delivered.

To prevent this, after the upgrade, you should remove the EMS LIF service from the network service polices that do not provide reachability to the destination.

Steps
1. Identify the LIFs and associated network service polices through which EMS messages can be sent:

   network interface show -fields service-policy -services management-ems

<table>
<thead>
<tr>
<th>vserver</th>
<th>lif</th>
<th>service-policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-1</td>
<td>cluster_mgmt</td>
<td>default-management</td>
</tr>
<tr>
<td>cluster-1</td>
<td>node1_mgmt</td>
<td>default-management</td>
</tr>
<tr>
<td>cluster-1</td>
<td>node2_mgmt</td>
<td>default-management</td>
</tr>
<tr>
<td>cluster-1</td>
<td>inter_cluster</td>
<td>default-intercluster</td>
</tr>
</tbody>
</table>

   4 entries were displayed.

2. Check each LIF for connectivity to the EMS destination:

   network ping -lif lif_name -vserver svm_name -destination destination_address

Perform this on each node.

Examples

   cluster-1::> network ping -lif node1-mgmt -vserver cluster-1 -destination 10.10.10.10
   10.10.10.10 is alive

   cluster-1::> network ping -lif inter_cluster -vserver cluster-1 -destination 10.10.10.10
   no answer from 10.10.10.10

3. Enter advanced privilege level:
set advanced

4. For the LIFs that do not have reachability, remove the management-ems LIF service from the corresponding service policies:

```
   network interface service-policy remove-service -vserver svm_name
            -policy service_policy_name -service management-ems
```

5. Verify that the management-ems LIF is now only associated with the LIFs that provide reachability to the EMS destination:

```
   network interface show -fields service-policy -services management-ems
```

Related Links

LIFs and service polices in ONTAP 9.6 and later

Verify networking and storage status for MetroCluster configurations after an ONTAP upgrade

After you upgrade an ONTAP cluster in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

1. Verify the LIF status:

```
   network interface show
```

In normal operation, LIFs for source SVMs must have an admin status of up and be located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs have an admin status of up, but they do not need to be located on their home nodes.
cluster1::> network interface show

<table>
<thead>
<tr>
<th>Logical</th>
<th>Status</th>
<th>Network</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vserver</td>
<td>Interface</td>
<td>Admin/Oper Address/Mask</td>
<td>Node</td>
</tr>
<tr>
<td>Home</td>
<td>--------</td>
<td>-------------------</td>
<td>------</td>
</tr>
</tbody>
</table>

```
----------- ---------- ---------- ------------------ --------------
------- ----
Cluster

cluster1-a1_clus1
  up/up  192.0.2.1/24       cluster1-01
true
e2a

c
cluster1-a1_clus2
  up/up  192.0.2.2/24       cluster1-01
true
e2b

c
cluster1-01
  clus_mgmt up/up  198.51.100.1/24    cluster1-01
true
e3a

cluster1-01
  clus_mgmt up/up  198.51.100.2/24    cluster1-01
true
e3c

...  

27 entries were displayed.
```

2. Verify the state of the aggregates:

```bash
storage aggregate show -state !online
```

This command displays any aggregates that are not online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

This example shows a cluster in normal operation:

```bash
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are
offline:

```
classroom::> storage aggregate show -state !online
Aggregate     Size Available Used% State   #Vols Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
----------
aggr0_b1
       0B   0B   0% offline 0 cluster2-01
raid_dp,
mirror
degraded
aggr0_b2
       0B   0B   0% offline 0 cluster2-02
raid_dp,
mirror
degraded
2 entries were displayed.
```

3. Verify the state of the volumes:

```
volume show -state !online
```

This command displays any volumes that are not online.

If the MetroCluster configuration is in normal operation (it is not in switchover state), the output should show all volumes owned by the cluster's secondary SVMs (those with the SVM name appended with "-mc").

Those volumes come online only in the event of a switchover.

This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.
cluster1::> volume show -state !online
(volume show)

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Aggregate</th>
<th>State</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Available</td>
<td>Used</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

--------- ----------- ------------ ---------- ----  ----------
---------- -----

vs2-mc    vol1    aggr1_b1  -    RW     -
          -   -

vs2-mc    root_vs2 aggr0_b1  -    RW     -
          -   -

vs2-mc    vol2    aggr1_b1  -    RW     -
          -   -

vs2-mc    vol3    aggr1_b1  -    RW     -
          -   -

vs2-mc    vol4    aggr1_b1  -    RW     -
          -   -

5 entries were displayed.

4. Verify that there are no inconsistent volumes:

    volume show -is-inconsistent true

See the Knowledge Base article Volume Showing WAFL Inconsistent on how to address the inconsistent volumes.

Verify the SAN configuration after an upgrade

After an ONTAP upgrade, in a SAN environment, you should verify that each initiator that was connected to a LIF before the upgrade has successfully reconnected to the LIF.

1. Verify that each initiator is connected to the correct LIF.

   You should compare the list of initiators to the list you made during the upgrade preparation.

<table>
<thead>
<tr>
<th>For...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>iSCSI</td>
<td>iscsi initiator show -fields igroup,initiator-name,tpgroup</td>
</tr>
<tr>
<td>FC</td>
<td>fcp initiator show -fields igroup,wwpn,lif</td>
</tr>
</tbody>
</table>
Reconfigure KMIP server connections after an upgrade from ONTAP 9.2 or earlier

After you upgrade from ONTAP 9.2 or earlier to ONTAP 9.3 or later, you need to reconfigure any external key management (KMIP) server connections.

Steps

1. Configure the key manager connectivity:

   `security key-manager setup`

2. Add your KMIP servers:

   `security key-manager add -address key_management_server_ip_address`

3. Verify that KMIP servers are connected:

   `security key-manager show -status`

4. Query the key servers:

   `security key-manager query`

5. Create a new authentication key and passphrase:

   `security key-manager create-key -prompt-for-key true`

   The passphrase must have a minimum of 32 characters.

6. Query the new authentication key:

   `security key-manager query`

7. Assign the new authentication key to your self-encrypting disks (SEDs):

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   Make sure you are using the new authentication key from your query.

8. If needed, assign a FIPS key to the SEDs:
If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

**Relocate moved load-sharing mirror source volumes after an ONTAP upgrade**

After you upgrade ONTAP, you need to move load-sharing mirror source volumes back to their pre-upgrade locations.

**Steps**

1. Identify the location to which you are moving the load-sharing mirror source volume by using the record you created before moving the load-sharing mirror source volume.
2. Move the load-sharing mirror source volume back to its original location:

   ```
   volume move start
   ```

**Resume SnapMirror operations after an ONTAP upgrade**

After an ONTAP upgrade, you need to resume any SnapMirror relationships that were suspended.

**Steps**

1. Resume transfers for each SnapMirror relationship that was previously quiesced:

   ```
   snapmirror resume *
   ```

   This command resumes the transfers for all quiesced SnapMirror relationships.
2. Verify that the SnapMirror operations have resumed:

   ```
   snapmirror show
   ```
cluster1::> snapmirror show

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Mirror</th>
<th>Relationship</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Path</td>
<td>Type</td>
<td>Path</td>
<td>State</td>
<td>Status</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
<td>--------</td>
<td>--------------</td>
<td>-------</td>
</tr>
<tr>
<td>clus1-clus1:dp_src1</td>
<td>DP</td>
<td>clus1-clus2:dp_dst1</td>
<td>Snapmirrored</td>
<td>Idle</td>
</tr>
<tr>
<td>clus1-clus1:xdp_src1</td>
<td>XDP</td>
<td>clus1-clus2:xdp_dst1</td>
<td>Snapmirrored</td>
<td>Idle</td>
</tr>
<tr>
<td>clus1:clus1-clus1:ls_src1</td>
<td>LS</td>
<td>clus1:clus1-clus1:ls_mr1</td>
<td>Snapmirrored</td>
<td>Idle</td>
</tr>
<tr>
<td>clus1:clus1-clus1:ls_mr2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 entries were displayed.

For each SnapMirror relationship, verify that the Relationship Status is Idle. If the status is Transferring, wait for the SnapMirror transfer to complete, and then reenter the command to verify that the status has changed to Idle.

For each SnapMirror relationship that is configured to run on a schedule, you should verify that the first scheduled SnapMirror transfer completes successfully.

Change in user accounts that can access the Service Processor

If you created user accounts in ONTAP 9.8 or earlier that can access the Service Processor (SP) with a non-admin role and you upgrade to ONTAP 9.9.1 or later, any non-admin value in the -role parameter is modified to admin.

For more information, see Accounts that can access the SP.

Update the Disk Qualification Package

After you upgrade your ONTAP software, you should download and install the ONTAP Disk Qualification Package (DQP). The DQP is not updated as part of an ONTAP upgrade.

The DQP contains the proper parameters for ONTAP interaction with all newly qualified drives. If your version
of the DQP does not contain information for a newly qualified drive, ONTAP will not have the information to properly configure the drive.

It is best practice to update the DQP every quarter. You should also update the DQP for the following reasons:

• Whenever you add a new drive type or size to a node in your cluster

For example, if you already have 1-TB drives and add 2-TB drives, you need to check for the latest DQP update.

• Whenever you update the disk firmware

• Whenever newer disk firmware or DQP files are available

**Related information**

- NetApp Downloads: Disk Qualification Package
- NetApp Downloads: Disk Drive Firmware

## Firmware and system updates

### Firmware and system updates overview

Depending upon your version of ONTAP, you can enable automatic firmware and system updates.

<table>
<thead>
<tr>
<th>ONTAP Version</th>
<th>What's included in automatic updates</th>
</tr>
</thead>
</table>
| 9.13.1 and later  | • ONTAP Time Zone Database  
|                   | • Storage firmware for storage devices, disks, and disk shelves  
|                   | • SP/BMC firmware for service processors and BMC modules                      |
| 9.10.1 and later  | • Storage firmware for storage devices, disks, and disk shelves  
|                   | • SP/BMC firmware for service processors and BMC modules                      |
| 9.9.1 and earlier | Not supported                                                                 |

If you are running ONTAP 9.9.1 or earlier, or if you do not have automatic system updates enabled, you can make firmware updates manually.

If you are running ONTAP 9.12.1 or earlier, or if you do not have automatic system updates enabled, you can update the Time Zone Database manually. See the Knowledge Base article, [How to update time zone information in ONTAP 9](#), for details.

**Video: Automatic firmware update feature**

Take a look at the automatic firmware update feature available starting in ONTAP 9.10.1.
How automatic updates are scheduled for installation

All eligible nodes within the same cluster are grouped together for automatic updates. The timeframe in which the eligible nodes are scheduled for automatic update varies based upon the priority level of the update and the percentage of systems in your environment that require the update.

For example, if 10% or less of your total systems are eligible for a non-priority update, the update is scheduled for all eligible systems within 1 week. However, if 76% or more of your total systems are eligible for a non-priority update, then the update is staggered across the eligible systems over the course of 8 weeks. This staggered installation helps to mitigate risks to your overall environment if there is an issue with an update that needs to be remedied.

The percentage of your total systems scheduled for automatic updates by week are as follows:

### For critical updates

<table>
<thead>
<tr>
<th>% of systems requiring update</th>
<th>% of updates that occur week 1</th>
<th>% of updates that occur week 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>50% or less</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>50-100%</td>
<td>30%</td>
<td>70%</td>
</tr>
</tbody>
</table>

### For high priority updates

<table>
<thead>
<tr>
<th>% of systems requiring update</th>
<th>% of updates that occur by week</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>week 1</td>
</tr>
<tr>
<td>25% or less</td>
<td>100%</td>
</tr>
<tr>
<td>% of systems requiring update</td>
<td>% of updates that occur by week</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>26-50%</td>
<td>30%</td>
</tr>
<tr>
<td>50-100%</td>
<td>10%</td>
</tr>
</tbody>
</table>

For normal priority updates

<table>
<thead>
<tr>
<th>% of systems requiring update</th>
<th>% of updates that occur by week</th>
<th>week 1</th>
<th>week 2</th>
<th>week 3</th>
<th>week 4</th>
<th>week 5</th>
<th>week 6</th>
<th>week 7</th>
<th>week 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>10% or less</td>
<td>100%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11-20%</td>
<td>30%</td>
<td>70%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21-50%</td>
<td>10%</td>
<td>20%</td>
<td>30%</td>
<td>40%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>51-75%</td>
<td>5%</td>
<td>10%</td>
<td>15%</td>
<td>20%</td>
<td>20%</td>
<td>30%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>76-100%</td>
<td>5%</td>
<td>5%</td>
<td>10%</td>
<td>10%</td>
<td>15%</td>
<td>15%</td>
<td>20%</td>
<td>20%</td>
<td></td>
</tr>
</tbody>
</table>

**Enable automatic updates**

Beginning with ONTAP 9.10.1, you can enable automatic updates to allow ONTAP to download and install firmware updates without your intervention.

Beginning in ONTAP 9.13.1, these automatic updates also include automatic Time Zone Database updates.

**Before you begin**

You must have a current support entitlement. This can be validated on the NetApp support site in the System Details page.

**About this task**

To enable automatic updates, you must first enable AutoSupport with HTTPs. If AutoSupport is not enabled on your cluster, or if AutoSupport is enabled on your cluster with another transport protocol, you will be given the option to enable it with HTTPs during this procedure.

**Steps**

1. In System Manager, click Events.
2. In the Overview section, next to Enable automatic update, click Actions>Enable.
3. If you do not have AutoSupport with HTTPs enabled, select to enable it.
4. Accept the terms and conditions and select Save.

**Related information**

Troubleshoot AutoSupport message delivery over HTTP or HTTPS
Modify automatic updates

When automatic updates are enabled, by default, ONTAP automatically detects, downloads, and installs all recommended firmware updates and, beginning with ONTAP 9.13.1, ONTAP Time Zone Database updates. If you would like to view recommended updates before they are installed, or if you would like to have the recommendations automatically dismissed, you can modify the default behavior to your preference.

Steps
1. In System Manager, click **Cluster > Settings**.
2. In the **Automatic Update** section, click ☰ to view a list of actions.
3. Click **Edit Automatic Update Settings**.
4. Specify the default actions to be taken for each event type.

You can choose to automatically update, show notifications, or automatically dismiss the updates for each event type.

> The ONTAP Time Zone database is controlled by the SYSTEM FILES event type.

Manage recommended automatic updates

The automatic update log displays a list of update recommendations and details about each one, including a description, category, scheduled time to install, status, and any errors. You can view the log and then decide what action you would like to perform for each recommendation.

Steps
1. View the list of recommendations:

<table>
<thead>
<tr>
<th>View from Cluster settings</th>
<th>View from the Firmware Update tab</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Click <strong>Cluster &gt; Settings</strong>.</td>
<td>a. Click <strong>Cluster &gt; Overview</strong>.</td>
</tr>
<tr>
<td>b. In the <strong>Automatic Update</strong> section, click ☰, then click <strong>View All Automatic Updates</strong>.</td>
<td>b. In the <strong>Overview</strong> section, click <strong>More ☰</strong>, then click <strong>ONTAP Update</strong>.</td>
</tr>
<tr>
<td>c. Select the <strong>Firmware Update</strong> tab.</td>
<td>c. Select the <strong>Firmware Update</strong> tab.</td>
</tr>
<tr>
<td>d. On the <strong>Firmware Update</strong> tab, click <strong>More ☰</strong>, then click <strong>View All Automatic Updates</strong>.</td>
<td>d. On the <strong>Firmware Update</strong> tab, click <strong>More ☰</strong>, then click <strong>View All Automatic Updates</strong>.</td>
</tr>
</tbody>
</table>

2. Click ☰ next to the description to view a list of actions you can perform on the recommendation.

You can perform one of the following actions, depending on the state of the recommendation:

<table>
<thead>
<tr>
<th>If the update is in this state…</th>
<th>You can…</th>
</tr>
</thead>
</table>


### Update firmware manually

Beginning with ONTAP 9.9.1, if you are registered with [Active IQ Unified Manager](https://www.netapp.com/products/active-iq-unified-manager), you can receive alerts in System Manager that inform you when firmware updates for supported devices, such as disk, disk shelves, the service processor (SP), or the Baseboard Management Controller (BMC) are pending on the cluster.

If you are running ONTAP 9.8 or you are not registered with Active IQ Unified Manager, you can navigate to the NetApp Support Site to download firmware updates.

#### Before you begin

To prepare for a smooth firmware update, you should reboot the SP or BMC before the update begins. You can use the `system service-processor reboot-sp -node node_name` command to reboot.

#### Steps

Follow the appropriate procedure based upon your version of ONTAP and if you are registered with Active IQ Unified Manager.
ONTAP 9.9.1 and later with Active IQ
1. In System Manager, go to Dashboard.
   
   In the Health section, a message displays if there are any recommended firmware updates for the cluster.

2. Click on the alert message.
   
   The Firmware Update tab is displayed in the Update page.

3. Click Download from NetApp Support Site for the firmware update that you want to perform.
   
   The NetApp Support Site is displayed.

4. Log into the NetApp Support Site and download the firmware image package needed for the update.

5. Copy the files to an HTTP or FTP server on your network or to a local folder.

6. In System Manager, click Cluster > Overview.

7. In the right corner of the Overview pane, click More and select ONTAP Update.

8. Click Firmware Update.

9. Depending on your version of ONTAP do the following:

<table>
<thead>
<tr>
<th>ONTAP 9.9.1 and 9.10.0</th>
<th>ONTAP 9.10.1 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Select From Server or Local Client</td>
<td>a. In the list of recommended updates, select Actions.</td>
</tr>
<tr>
<td>b. Provide the server URL or the file location.</td>
<td>b. Click Update to install the update immediately or Schedule to schedule it for later.</td>
</tr>
<tr>
<td></td>
<td>If the update is already scheduled, you can Edit or Cancel it.</td>
</tr>
<tr>
<td></td>
<td>c. Select the Update Firmware button.</td>
</tr>
</tbody>
</table>

ONTAP 9.8 and later without Active IQ
1. Navigate to the NetApp Support Site and log in.

2. Select the firmware package that you want to use to update your cluster firmware.

3. Copy the files to an HTTP or FTP server on your network or to a local folder.

4. In System Manager, click Cluster > Overview.

5. In the right corner of the Overview pane, click More and select ONTAP Update.

6. Click Firmware Update.

7. Depending on your version of ONTAP do the following:
After you finish
You can monitor or verify updates under Firmware Update Summary. To view updates that were dismissed or failed to install click Cluster > Settings > Automatic Update > View All Automatic Updates.

Revert ONTAP

Revert ONTAP overview
To transition a cluster to an earlier ONTAP release, you must perform a reversion.

The information in this section will guide you through the steps you should take before and after you revert, including the resources you should read and the necessary pre- and post-revert checks you should perform.

Do I need technical support to revert?
You can revert without assistance on new or test clusters. You should call technical support to revert production clusters. You should also call technical support if you experience any of the following:

- You are in a production environment and revert fails or you encounter any problems before or after the revert such as:
  - The revert process fails and cannot finish.
  - The revert process finishes, but the cluster is unusable in a production environment.
  - The revert process finishes and the cluster goes into production, but you are not satisfied with its behavior.

- You created volumes in ONTAP 9.5 or later and you need to revert to an earlier version. Volumes using adaptive compression must be uncompressed before reverting.

Revert paths
The version of ONTAP that you can revert to varies based on the version of ONTAP currently running on your nodes. You can use the system image show command to
determine the version of ONTAP running on each node.

These guidelines refer only to on-premises ONTAP releases. For information about reverting ONTAP in the cloud, see Reverting or downgrading Cloud Volumes ONTAP.

<table>
<thead>
<tr>
<th>You can revert from…</th>
<th>To…</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP 9.13.1</td>
<td>ONTAP 9.12.1</td>
</tr>
<tr>
<td>ONTAP 9.12.1</td>
<td>ONTAP 9.11.1</td>
</tr>
<tr>
<td>ONTAP 9.11.1</td>
<td>ONTAP 9.10.1</td>
</tr>
<tr>
<td>ONTAP 9.10.1</td>
<td>ONTAP 9.9.1</td>
</tr>
<tr>
<td>ONTAP 9.9.1</td>
<td>ONTAP 9.8</td>
</tr>
<tr>
<td>ONTAP 9.8</td>
<td>ONTAP 9.7</td>
</tr>
<tr>
<td>ONTAP 9.7</td>
<td>ONTAP 9.6</td>
</tr>
<tr>
<td>ONTAP 9.6</td>
<td>ONTAP 9.5</td>
</tr>
<tr>
<td>ONTAP 9.5</td>
<td>ONTAP 9.4</td>
</tr>
<tr>
<td>ONTAP 9.4</td>
<td>ONTAP 9.3</td>
</tr>
<tr>
<td>ONTAP 9.3</td>
<td>ONTAP 9.2</td>
</tr>
<tr>
<td>ONTAP 9.2</td>
<td>ONTAP 9.1</td>
</tr>
<tr>
<td>ONTAP 9.1 or ONTAP 9</td>
<td>Data ONTAP 8.3.x</td>
</tr>
</tbody>
</table>

If you need to change from ONTAP 9.1 to 9.0, you should follow the downgrade process documented here.

What should I read before I revert?

Resources to review before you revert

Before you revert ONTAP, you should confirm hardware support and review resources to understand issues you might encounter or need to resolve.

1. Review the ONTAP 9 Release Notes for the target release.
The “Important cautions” section describes potential issues that you should be aware of before downgrading or reverting.

2. Confirm that your hardware platform is supported in the target release.

NetApp Hardware Universe

3. Confirm that your cluster and management switches are supported in the target release.

You must verify that the NX-OS (cluster network switches), IOS (management network switches), and reference configuration file (RCF) software versions are compatible with the version of ONTAP to which you are reverting.

NetApp Downloads: Cisco Ethernet Switch

4. If your cluster is configured for SAN, confirm that the SAN configuration is fully supported.

All SAN components—including target ONTAP software version, host OS and patches, required Host Utilities software, and adapter drivers and firmware—should be supported.

NetApp Interoperability Matrix Tool

Revert considerations

You need to consider the revert issues and limitations before beginning an ONTAP reversion.

- Reversion is disruptive.

No client access can occur during the reversion. If you are reverting a production cluster, be sure to include this disruption in your planning.

- Reversion affects all nodes in the cluster.

The reversion affects all nodes in the cluster; however, the reversion must be performed and completed on each HA pair before other HA pairs are reverted.

- The reversion is complete when all nodes are running the new target release.

When the cluster is in a mixed-version state, you should not enter any commands that alter the cluster operation or configuration except as necessary to satisfy reversion requirements; monitoring operations are permitted.

If you have reverted some, but not all of the nodes, do not attempt to upgrade the cluster back to the source release.

- When you revert a node, it clears the cached data in a Flash Cache module.

Because there is no cached data in the Flash Cache module, the node serves initial read requests from disk, which results in decreased read performance during this period. The node repopulates the cache as it serves read requests.

- A LUN that is backed up to tape running on ONTAP 9.x can be restored only to 9.x and later releases and not to an earlier release.
• If your current version of ONTAP supports In-Band ACP (IBACP) functionality, and you revert to a version of ONTAP that does not support IBACP, the alternate path to your disk shelf is disabled.

• If LDAP is used by any of your storage virtual machines (SVMs), LDAP referral must be disabled before reversion.

• In MetroCluster IP systems using switches which are MetroCluster compliant but not MetroCluster validated, the reversion from ONTAP 9.7 to 9.6 is disruptive as there is no support for systems using ONTAP 9.6 and earlier.

**Things to verify before you revert**

Before revert, you should verify your cluster health, storage health, and system time. You should also delete any cluster jobs that are running and gracefully terminate any SMB sessions that are not continuously available.

**Verify cluster health**

Before you revert cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster: `cluster show`

```
cluster1::> cluster show
```

<table>
<thead>
<tr>
<th>Node</th>
<th>Health</th>
<th>Eligibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>node1</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:

```
set -privilege advanced
```

Enter y to continue.

3. Verify the configuration details for each RDB process.
   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.

   Note that each ring might have a different quorum master.

<table>
<thead>
<tr>
<th>To display this RDB process...</th>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management application</td>
<td>cluster ring show -unitname mgmt</td>
</tr>
<tr>
<td>Volume location database</td>
<td>cluster ring show -unitname vldb</td>
</tr>
<tr>
<td>Virtual-Interface manager</td>
<td>cluster ring show -unitname vifmgr</td>
</tr>
</tbody>
</table>
To display this RDB process...
SAN management daemon

<table>
<thead>
<tr>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster ring show -unitname bcomd</td>
</tr>
</tbody>
</table>

This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node  UnitName Epoch  DB Epoch  DB Trnxs  Master     Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Return to the admin privilege level:
```
set -privilege admin
```

5. If you are operating in a SAN environment, verify that each node is in a SAN quorum:
```
event log show -severity informational -message-name scsiblade.*
```

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show -severity informational -message-name scsiblade.*
Time             Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
               node1      INFORMATIONAL  scsiblade.in.quorum: The

Related information
System administration

Verify storage health

Before you revert a cluster, you should verify the status of your disks, aggregates, and volumes.

1. Verify disk status:
<table>
<thead>
<tr>
<th>To check for...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broken disks</td>
<td>a. Display any broken disks: storage disk show -state broken</td>
</tr>
<tr>
<td></td>
<td>b. Remove or replace any broken disks.</td>
</tr>
<tr>
<td>Disks undergoing maintenance or reconstruction</td>
<td>a. Display any disks in maintenance, pending, or reconstructing states:</td>
</tr>
<tr>
<td></td>
<td>storage disk show -state maintenance</td>
</tr>
<tr>
<td></td>
<td>b. Wait for the maintenance or reconstruction operation to finish before</td>
</tr>
<tr>
<td></td>
<td>proceeding.</td>
</tr>
</tbody>
</table>

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates: `storage aggregate show -state !online`

   This command displays the aggregates that are not online. All aggregates must be online before and after performing a major upgrade or reversion.

   ```bash
   cluster1::> storage aggregate show -state !online
   There are no entries matching your query.
   ```

3. Verify that all volumes are online by displaying any volumes that are not online: `volume show -state !online`

   All volumes must be online before and after performing a major upgrade or reversion.

   ```bash
   cluster1::> volume show -state !online
   There are no entries matching your query.
   ```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

   See the Knowledge Base article [Volume Showing WAFL Inconsistent](#) on how to address the inconsistent volumes.

**Related information**

**Disk and aggregate management**

**Verifying the system time**

Before you revert, you should verify that NTP is configured, and that the time is synchronized across the cluster.

1. Verify that the cluster is associated with an NTP server: `cluster time-service ntp server show`
2. Verify that each node has the same date and time: `cluster date show`
Verify that no jobs are running

Before you revert the ONTAP software, you must verify the status of cluster jobs. If any aggregate, volume, NDMP (dump or restore), or Snapshot jobs (such as create, delete, move, modify, replicate, and mount jobs) are running or queued, you must allow the jobs to finish successfully or stop the queued entries.

1. Review the list of any running or queued aggregate, volume, or Snapshot jobs: `job show`

   ```
   cluster1::> job show
   Owning Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   8629   Vol Reaper           cluster1   -              Queued
            Description: Vol Reaper Job
   8630   Certificate Expiry Check
            cluster1   -              Queued
            Description: Certificate Expiry Check
   ```

2. Delete any running or queued aggregate, volume, or Snapshot copy jobs: `job delete -id job_id`

   ```
   cluster1::> job delete -id 8629
   ```

3. Verify that no aggregate, volume, or Snapshot jobs are running or queued: `job show`

   ```
   In this example, all running and queued jobs have been deleted:
   ```
SMB sessions that should be terminated

Before you revert, you should identify and gracefully terminate any SMB sessions that are not continuously available.

Continuously available SMB shares, which are accessed by Hyper-V or Microsoft SQL Server clients using the SMB 3.0 protocol, do not need to be terminated before upgrading or downgrading.

1. Identify any established SMB sessions that are not continuously available: `vserver cifs session show -continuously-available No -instance`

   This command displays detailed information about any SMB sessions that have no continuous availability. You should terminate them before proceeding with the ONTAP downgrade.
2. If necessary, identify the files that are open for each SMB session that you identified:

```bash
vserver cifs session file show -session-id session_ID
```

```
cluster1::> vserver cifs session file show -session-id 1
``` 

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Mode</th>
<th>Volume</th>
<th>Share</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Regular</td>
<td>rw</td>
<td>vol10</td>
<td>homedirshare</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Path: \\TestDocument.docx

Path: \\file1.txt

2 entries were displayed.

**NVMe in-band authentication**

If you are reverting from ONTAP 9.12.1 or later to ONTAP 9.12.0 or earlier, you must **disable in-band**
authentication before you revert. If in-band authentication using DH-HMAC-CHAP is not disabled, revert will fail.

What else should I check before I revert?

Pre-revert checks

Depending on your environment, you need to consider certain factors before revert. Get started by reviewing the table below to see what special considerations you need to consider.

<table>
<thead>
<tr>
<th>Ask yourself…</th>
<th>If your answer is yes, then do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is my cluster running SnapMirror?</td>
<td>• Review considerations for reverting systems with SnapMirror Synchronous relationships</td>
</tr>
<tr>
<td></td>
<td>• Review reversion requirements for SnapMirror and SnapVault relationships</td>
</tr>
<tr>
<td>Is my cluster running SnapLock?</td>
<td>Set autocommit periods</td>
</tr>
<tr>
<td>Do I have Split FlexClone volumes?</td>
<td>Reverse physical block sharing</td>
</tr>
<tr>
<td>Do I have FlexGroup volumes?</td>
<td>Disable qtree functionality</td>
</tr>
<tr>
<td>Do I have CIFS servers in workgroup mode?</td>
<td>Move or delete CIFS servers in workgroup mode</td>
</tr>
<tr>
<td>Do I have deduplicated volumes?</td>
<td>Verify volume contains enough free space</td>
</tr>
<tr>
<td>Do I have Snapshot copies?</td>
<td>Prepare Snapshop copies</td>
</tr>
<tr>
<td>Am I reverting to ONTAP 8.3.x?</td>
<td>Identify user accounts that use SHA-2 hash function</td>
</tr>
<tr>
<td>Is anti-ransomware protection configured for ONTAP 9.11.1 or later?</td>
<td>Check anti-ransomware licensing</td>
</tr>
<tr>
<td>Is S3 multiprotocol access configured for ONTAP 9.12.1 or later?</td>
<td>Remove S3 NAS bucket configuration</td>
</tr>
<tr>
<td>Is NFSv4.1 session trunking configured for ONTAP 9.14.1 or later?</td>
<td>Remove NFSv4.1 session trunking configuration</td>
</tr>
</tbody>
</table>

MetroCluster pre-revert checks

Depending on your MetroCluster configuration, you need to consider certain factors before revert. Get started by reviewing the table below to see what special considerations you need to consider.

<table>
<thead>
<tr>
<th>Ask yourself…</th>
<th>If your answer is yes, then do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do I have a two- or four-node MetroCluster configuration?</td>
<td>Disable automatic unplanned switchover</td>
</tr>
<tr>
<td>Do I have a four- or eight-node MetroCluster IP or fabric-attached configuration running ONTAP 9.12.1 or later?</td>
<td>Disable IPsec</td>
</tr>
</tbody>
</table>
SnapMirror

Considerations for reverting systems with SnapMirror Synchronous relationships

You must be aware of the considerations for SnapMirror Synchronous relationships before reverting from ONTAP 9.6 to ONTAP 9.5.

Before reverting, you must take the following steps if you have SnapMirror Synchronous relationships:

• You must delete any SnapMirror Synchronous relationship in which the source volume is serving data using NFSv4 or SMB.

  ONTAP 9.5 does not support NFSv4 and SMB.

• You must delete any SnapMirror Synchronous relationships in a mirror-mirror cascade deployment.

  A mirror-mirror cascade deployment is not supported for SnapMirror Synchronous relationships in ONTAP 9.5.

• If the common Snapshot copies in ONTAP 9.5 are not available during revert, you must initialize the SnapMirror Synchronous relationship after reverting.

  After two hours of upgrade to ONTAP 9.6, the common Snapshot copies from ONTAP 9.5 are automatically replaced by the common Snapshot copies in ONTAP 9.6. Therefore, you cannot resynchronize the SnapMirror Synchronous relationship after reverting if the common Snapshot copies from ONTAP 9.5 are not available.

Reversion requirements for SnapMirror and SnapVault relationships

The system node revert-to command notifies you of any SnapMirror and SnapVault relationships that need to be deleted or reconfigured for the reversion process to be completed. However, you should be aware of these requirements before you begin the reversion.

• All SnapVault and data protection mirror relationships must be quiesced and then broken.

  After the reversion is completed, you can resynchronize and resume these relationships if a common Snapshot copy exists.

• SnapVault relationships must not contain the following SnapMirror policy types:

  ◦ async-mirror

    You must delete any relationship that uses this policy type.

  ◦ MirrorAndVault

    If any of these relationships exist, you should change the SnapMirror policy to mirror-vault.

• All load-sharing mirror relationships and destination volumes must be deleted.

• SnapMirror relationships with FlexClone destination volumes must be deleted.

• Network compression must be disabled for each SnapMirror policy.

• The all_source_snapshot rule must be removed from any async-mirror type SnapMirror policies.
The Single File Snapshot Restore (SFSR) and Partial File Snapshot Restore (PFSR) operations are deprecated on the root volume.

- Any currently running single file and Snapshot restore operations must be completed before the reversion can proceed.

  You can either wait for the restore operation to finish, or you can abort it.

- Any incomplete single file and Snapshot restore operations must be removed by using the snapmirror restore command.

Set autocommit periods for SnapLock volumes before reverting

To revert from ONTAP 9, the value of the autocommit period for SnapLock volumes must be set in hours, not days. Before attempting to revert, you must check the autocommit value for your SnapLock volumes and modify it from days to hours, if necessary.

1. Verify that there are SnapLock volumes in the cluster that have unsupported autocommit periods:
   ```bash
   volume snaplock show -autocommit-period *days
   ```

2. Modify the unsupported autocommit periods to hours:
   ```bash
   volume snaplock modify -vserver vserver_name -volume volume_name -autocommit-period value hours
   ```

Reverse physical block sharing in split FlexClone volumes

If you have split a FlexClone volume from its parent volume, you must undo the sharing of any physical block between the clone and its parent volume before reverting from ONTAP 9.4 or later to an earlier version of ONTAP.

This task is applicable only for AFF systems when split has been run on any of the FlexClone volumes.

1. Log in to the advanced privilege level:
   ```bash
   set -privilege advanced
   ```

2. Identify the split FlexClone volumes with shared physical blocks:
   ```bash
   volume clone sharing-by-split show
   ```

   ```text
   cluster1::> volume clone sharing-by-split show
   Node   Vserver   Volume        Aggregate
   -------------- ------------- -------------- --------------
   node1       vs1       vol_clone1    aggr1
   node2       vs2       vol_clone2    aggr2
   2 entries were displayed.
   ```

3. Undo the physical block sharing in all of the split FlexClone volumes across the cluster:
   ```bash
   volume clone sharing-by-split undo start-all
   ```

4. Verify that there are no split FlexClone volumes with shared physical blocks:
   ```bash
   volume clone sharing-by-split show
   ```
Disable qtree functionality in FlexGroup volumes before reverting

Qtrees for FlexGroup volumes are not supported prior to ONTAP 9.3. You must disable the qtree functionality on FlexGroup volumes before reverting from ONTAP 9.3 to an earlier version of ONTAP.

The qtree functionality is enabled either when you create a qtree or if you modify the security-style and oplock-mode attributes of the default qtree.

1. Identify and delete all of the non-default qtrees in each FlexGroup volume that are enabled with the qtree functionality:
   a. Log in to the advanced privilege level: `set -privilege advanced`
   b. Verify if any FlexGroup volume is enabled with the qtree functionality.
      
      For ONTAP 9.6 or later, use: `volume show -is-qtree-caching-enabled true`
      
      For ONTAP 9.5 or earlier, use: `volume show -is-flexgroup-qtree-enabled true`

      ```
      cluster1::*> volume show -is-flexgroup-qtree-enabled true
      Vserver Volume Aggregate State Type Size
      Available Used% 
      -------------------------- ---------- ---- ----------
      --------- ----- 
      vs0 fg - online RW 320MB 220.4MB 31%
      ```

   c. Delete all of the non-default qtrees in each FlexGroup volume that are enabled with the qtree functionality: `volume qtree delete -vserver svm_name -volume volume_name -qtree qtree_name`
      
      If the qtree functionality is enabled because you modified the attributes of the default qtree and if you do not have any qtrees, you can skip this step.

      ```
      cluster1::*> volume qtree delete -vserver vs0 -volume fg -qtree qtree4
      WARNING: Are you sure you want to delete qtree qtree4 in volume fg
      vserver vs0?  {y|n}: y
      [Job 38] Job is queued: Delete qtree qtree4 in volume fg vserver vs0.
      ```

2. Disable the qtree functionality on each FlexGroup volume: `volume flexgroup qtree-disable -vserver svm_name -volume volume_name`
3. Identify and delete any Snapshot copies that are enabled with the qtree functionality.
   a. Verify if any Snapshot copies are enabled with the qtree functionality: `volume snapshot show -vserver vserver_name -volume volume_name -fields is-flexgroup-qtree-enabled`

   
   ```
   cluster1::*> volume snapshot show -vserver vs0 -volume fg -fields is-flexgroup-qtree-enabled
   vserver volume snapshot is-flexgroup-qtree-enabled
   ------- ------ -------- --------------------------
   vs0     fg     fg_snap1 true
   vs0     fg     daily.2017-09-27_0010 true
   vs0     fg     daily.2017-09-28_0010 true
   vs0     fg     snapmirror.0241f354-a865-11e7-a1c0-00a098a71764_2147867740.2017-10-04_124524 true
   ```

   b. Delete all of the Snapshot copies that are enabled with the qtree functionality: `volume snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot_name -force true -ignore-owners true`

   The Snapshot copies that must be deleted include regular Snapshot copies and the Snapshot copies taken for SnapMirror relationships. If you have created any SnapMirror relationship for the FlexGroup volumes with a destination cluster that is running ONTAP 9.2 or earlier, you must delete all of the Snapshot copies that were taken when the source FlexGroup volume was enabled for the qtree functionality.

   ```
   cluster1::> volume snapshot delete -vserver vs0 -volume fg -snapshot daily.2017-09-27_0010 -force true -ignore-owners true
   ```

**Related information**

**FlexGroup volumes management**

**Identify and move SMB servers in workgroup mode**

Before performing a revert, you must delete any SMB servers in workgroup mode or move them in to a domain. Workgroup mode is not supported on ONTAP versions prior to ONTAP 9.

1. Identify any SMB servers with a Authentication Style of workgroup: `vserver cifs show`

2. Move or delete the servers you identified:
### If you are going to... | Then use this command....
--- | ---
Move the SMB server from the workgroup to an Active Directory domain: | `vserver cifs modify -vserver vserver_name -domain domain_name`

Delete the SMB server | `vserver cifs delete -vserver vserver_name`

3. If you deleted the SMB server, enter the username of the domain, then enter the user password.

### Related information

**SMB management**

### Verify deduplicated volumes have enough free space before reverting

Before reverting from any version of ONTAP 9, you must ensure that the volumes contain sufficient free space for the revert operation.

The volume must have enough space to accommodate the savings that were achieved through the inline detection of blocks of zeros. See the Knowledge Base article [How to see space savings from deduplication, compression, and compaction in ONTAP 9](#).

If you have enabled both deduplication and data compression on a volume that you want to revert, then you must revert data compression before reverting deduplication.

1. Use the volume efficiency show command with the `-fields` option to view the progress of the efficiency operations that are running on the volumes.

   The following command displays the progress of efficiency operations: `volume efficiency show -fields vserver,volume,progress`

2. Use the volume efficiency stop command with the `-all` option to stop all active and queued deduplication operations.

   The following command stops all active and queued deduplication operations on volume VolA: `volume efficiency stop -vserver vs1 -volume VolA -all`

3. Use the set `-privilege advanced` command to log in at the advanced privilege level.

4. Use the volume efficiency revert-to command with the `-version` option to downgrade the efficiency metadata of a volume to a specific version of ONTAP.

   The following command reverts the efficiency metadata on volume VolA to ONTAP 9.x: `volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x`

   - The volume efficiency revert-to command reverts volumes that are present on the node on which this command is executed. This command does not revert volumes across nodes.

5. Use the volume efficiency show command with the `-op-status` option to monitor the progress of the downgrade.

   The following command monitors and displays the status of the downgrade: `volume efficiency show`
-vserver vs1 -op-status Downgrading

6. If the revert does not succeed, use the volume efficiency show command with the -instance option to see why the revert failed.

The following command displays detailed information about all fields: volume efficiency show
-vserver vs1 -volume vol1 -instance

7. After the revert operation is complete, return to the admin privilege level: set -privilege admin

Logical storage management

Prepare Snapshot copies before reverting

Before reverting to an earlier ONTAP release, you must disable all Snapshot copy policies and delete any Snapshot copies that were created after upgrading to the current release.

If you are reverting in a SnapMirror environment, you must first have deleted the following mirror relationships:

- All load-sharing mirror relationships
- Any data protection mirror relationships that were created in ONTAP 8.3.x
- All data protection mirror relationships if the cluster was re-created in ONTAP 8.3.x

1. Disable Snapshot copy policies for all data SVMs: volume snapshot policy modify -vserver * -enabled false

2. Disable Snapshot copy policies for each node’s aggregates:
   a. Identify the node’s aggregates by using the run-nodenodenameaggr status command.
   b. Disable the Snapshot copy policy for each aggregate: run -node nodename aggr options aggr_name nosnap on
   c. Repeat this step for each remaining node.

3. Disable Snapshot copy policies for each node’s root volume:
   a. Identify the node’s root volume by using the run-nodenodenodenamevol status command.

   You identify the root volume by the word root in the Options column of the vol status command output.

<table>
<thead>
<tr>
<th>vs1::&gt; run -node node1 vol status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume State</td>
</tr>
<tr>
<td>vol0 online</td>
</tr>
</tbody>
</table>

   b. Disable the Snapshot copy policy on the root volume: run -node nodename vol options root_volume_name nosnap on
   c. Repeat this step for each remaining node.
4. Delete all Snapshot copies that were created after upgrading to the current release:
   a. Set the privilege level to advanced: `set -privilege advanced`
   b. Disable the snapshots: `snapshot policy modify -vserver * -enabled false`
   c. Delete the node’s newer-version Snapshot copies: `volume snapshot prepare-for-revert -node nodename`

   This command deletes the newer-version Snapshot copies on each data volume, root aggregate, and root volume.

   If any Snapshot copies cannot be deleted, the command fails and notifies you of any required actions you must take before the Snapshot copies can be deleted. You must complete the required actions and then rerun the `volume snapshot prepare-for-revert` command before proceeding to the next step.

   ```bash
   cluster1::*> volume snapshot prepare-for-revert -node node1
   Warning: This command will delete all Snapshot copies that have the format used by the current version of ONTAP. It will fail if any Snapshot copy policies are enabled, or if any Snapshot copies have an owner. Continue? {y|n}: y
   ```

   d. Verify that the Snapshot copies have been deleted: `volume snapshot show -node nodename`

   If any newer-version Snapshot copies remain, force them to be deleted: `volume snapshot delete {-fs-version 9.0 -node nodename -is-constituent true} -ignore -owners -force`

e. Repeat this step c for each remaining node.

f. Return to the admin privilege level: `set -privilege admin`

   You must perform these steps on both the clusters in MetroCluster configuration.

**Identify user accounts that use SHA-2 hash function**

If you are reverting from ONTAP 9.1 or ONTAP 9.0 to ONTAP 8.3.x, SHA-2 account users can no longer be authenticated with their passwords. Before you revert, you should identify the user accounts that use the SHA-2 hash function, so that after reverting, you can have them reset their passwords to use the encryption type (MD5) that is supported by the release you revert to.

1. Change to the privilege setting to advanced: `set -privilege advanced`

2. Identify the user accounts that use the SHA-2 has function: `security login show -vserver * -username * -application * -authentication-method password -hash-function !md5`

3. Retain the command output for use after the revert.
During the revert, you will be prompted to run the advanced command `security login password-prepare-to-downgrade` to reset your own password to use the MD5 hash function. If your password is not encrypted with MD5, the command prompts you for a new password and encrypts it with MD5, enabling your credential to be authenticated after the revert.

**Check Autonomous Ransomware Protection licensing before reverting from ONTAP 9.11.1 or later**

If you have configured Autonomous Ransomware Protection (ARP) and you revert from ONTAP 9.11.1 or later to ONTAP 9.10.1 or earlier, you might experience warning messages and limited ARP functionality.

In ONTAP 9.11.1, the Anti-ransomware license replaced the Multi-Tenant Key Management (MTKM) license. If your system has the Anti_ransomware license but no MT_EK_MGMT license, you will see a warning during revert that ARP cannot be enabled on new volumes upon revert.

The volumes with existing protection will continue to work normally after revert, and ARP status can be displayed using the ONTAP CLI. System Manager cannot show ARP status without the MTKM license.

Therefore, if you want ARP to continue after reverting to ONTAP 9.10.1, be sure the MTKM license is installed before reverting. Learn about ARP licensing.

**Remove S3 NAS bucket configuration before reverting from ONTAP 9.12.1 or later**

If you have configured S3 client access for NAS data, before you revert from ONTAP 9.12.1 or later to ONTAP 9.11.1 or earlier, you should use the ONTAP command line interface (CLI) to remove the NAS bucket configuration and to remove any name mappings (S3 users to Windows or Unix users).

**About this task**

The following tasks are completed in the background during the revert process.

- Remove all partially completed singleton object creations (that is, all entries in hidden directories).
- Remove all hidden directories; there might be one on for each volume that is accessible from the root of the export mapped from the S3 NAS bucket.
- Remove the upload table.
- Delete any default-unix-user and default-windows-user values for all configured S3 servers.

**Steps**

1. Remove S3 NAS bucket configuration:

   ```bash
   vserver object-store-server bucket delete -vserver _svm_name_ -bucket _s3_nas_bucket_name_
   ``

2. Remove name mappings for UNIX:

   ```bash
   vserver name-mapping delete -vserver _svm_name_ -direction s3-unix
   ```
3. Remove name mappings for Windows:

```bash
vserver name-mapping delete -vserver _svm_name_ -direction s3-win
```

4. Remove the S3 protocols from the SVM:

```bash
vserver remove-protocols -vserver <svm_name> -protocols s3
```

**Remove NFSv4.1 session trunking configuration before reverting from ONTAP 9.14.1 or later**

If you have enabled trunking for client connections and you revert to a release earlier to ONTAP 9.14.1, you must disable trunking on any NFSv4.1 servers before reverting.

When you enter the `revert-to` command, you will see a warning message advising you to disable trunking before proceeding.

After reverting to an earlier ONTAP release, the clients using trunked connections fall back to using a single connection. Their data throughput will be affected, but there will be no disruption. The revert behavior is the same as modifying the NFSv4.1 trunking option for the SVM from enabled to disabled.

**Steps**

1. Disable trunking on the NFSv4.1 server:
   ```bash
   vserver nfs modify -vserver svm_name -v4.1-trunking disabled
   ```

2. Verify that NFS is configured as desired:
   ```bash
   vserver nfs show -vserver svm_name
   ```

**Disable automatic unplanned switchover before reverting two-node and four-node MetroCluster configurations**

Before reverting a two-node or four-node MetroCluster configuration, you must disable automatic unplanned switchover (AUSO).

1. On both the clusters in MetroCluster, disable automatic unplanned switchover:
   ```bash
   metrocluster modify -auto-switchover-failure-domain auso-disabled
   ```

**Related information**

*MetroCluster management and disaster recovery*

**Disable IPsec before reverting MetroCluster configurations**

Before reverting a MetroCluster configuration, you must disable IPsec.

You cannot revert ONTAP in a MetroCluster configuration running ONTAP 9.12.1 with IPsec enabled. A check is performed before revert to ensure there are no IPsec configurations within the MetroCluster configuration. You must remove any IPsec configurations present and disable IPsec before continuing with the revert. Reverting ONTAP is blocked if IPsec is enabled, even when you have not configured any user policies.
Download and install the ONTAP software image

Related information
You must first download the ONTAP software from the NetApp Support site; then you can install it.

Download the software image
To downgrade or revert from ONTAP 9.4 and later, you can copy the ONTAP software image from the NetApp Support Site to a local folder. For a downgrade or revert to ONTAP 9.3 or earlier, you must copy the ONTAP software image to an HTTP server or FTP server on your network.

You should note the following important information:

• Software images are specific to platform models.
  You must obtain the correct image for your cluster. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site.

• Software images include the latest version of system firmware that was available when a given version of ONTAP was released.

• If you are downgrading a system with NetApp Volume Encryption from ONTAP 9.5 or later, you must download the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

  If you use the ONTAP software image for restricted countries to downgrade or revert a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

  1. Locate the target ONTAP software in the Software Downloads area of the NetApp Support Site.
  2. Copy the software image.

    ▪ For ONTAP 9.3 or earlier, copy the software image (for example, 93_q_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served.

    ▪ For ONTAP 9.4 or later, copy the software image (for example, 97_q_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served or to a local folder.

Install the software image
You must install the target software image on the cluster’s nodes.

• If you are downgrading or reverting a system with NetApp Volume Encryption from ONTAP 9.5 or later, you must have downloaded the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

  If you use the ONTAP software image for restricted countries to downgrade or revert a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

  1. Set the privilege level to advanced, entering `y` when prompted to continue: `set -privilege advanced`

     The advanced prompt (*>>) appears.
2. Install the software image on the nodes.

This command downloads and installs the software image on all of the nodes simultaneously. To download and install the image on each node one at a time, do not specify the -background parameter.

- If you are downgrading or reverting a non-MetroCluster configuration or a two-node MetroCluster configuration:

  ```
  system node image update -node * -package location -replace-package true -setdefault true -background true
  ```

  This command uses an extended query to change the target software image, which is installed as the alternate image, to be the default image for the node.

- If you are downgrading or reverting a four or eight-node MetroCluster configuration, you must issue the following command on both clusters:

  ```
  system node image update -node * -package location -replace-package true true -background true -setdefault false
  ```

  This command uses an extended query to change the target software image, which is installed as the alternate image on each node.

3. Enter `y` to continue when prompted.

4. Verify that the software image is downloaded and installed on each node:

  ```
  system node image show-update-progress -node *
  ```

  This command displays the current status of the software image download and installation. You should continue to run this command until all nodes report a Run Status of Exited, and an Exit Status of Success.

  The system node image update command can fail and display error or warning messages. After resolving any errors or warnings, you can run the command again.

  This example shows a two-node cluster in which the software image is downloaded and installed successfully on both nodes:

  ```
  cluster1::*> system node image show-update-progress -node *
  There is no update/install in progress
  Status of most recent operation:
    Run Status:     Exited
    Exit Status:    Success
    Phase:          Run Script
    Exit Message:   After a clean shutdown, image2 will be set as the default boot image on node0.
  There is no update/install in progress
  Status of most recent operation:
    Run Status:     Exited
    Exit Status:    Success
    Phase:          Run Script
    Exit Message:   After a clean shutdown, image2 will be set as the default boot image on node1.
  2 entries were acted on.
  ```
Revert an ONTAP cluster

To take the cluster offline to revert to an earlier ONTAP release, you must disable storage failover and the data LIFs, address reversion preconditions, revert the cluster and file system configurations on a node, and then repeat the process for each additional node in the cluster.

You must have completed the revert verifications and pre-checks.

Reverting a cluster requires you to take the cluster offline for the duration of the reversion.

1. Set the privilege level to advanced: `set -privilege advanced`
   
Enter `y` when prompted to continue.

2. Verify that the target ONTAP software is installed: `system image show`

   The following example shows that version 9.1 is installed as the alternate image on both nodes:

   ```
   cluster1:~*> system image show
   Is      Is                 Install
   Node     Image   Default Current Version    Date
   -------- ------- ------- ------- --------   -------------------
   node0     image1  true    true    9.2        MM/DD/YYYY TIME
             image2  false   false   9.1        MM/DD/YYYY TIME
   node1     image1  true    true    9.2        MM/DD/YYYY TIME
             image2  false   false   9.1        MM/DD/YYYY TIME
   4 entries were displayed.
   ```

3. Disable all of the data LIFs in the cluster: `network interface modify {-role data} -status -admin down`

4. Determine if you have inter-cluster flexcache relationships: `flexcache origin show-caches -relationship-type inter-cluster`

5. If inter-cluster flexcaches are present, disable the data lifs on the cache cluster: `network interface modify -vserver vserver_name -lif lif_name -status-admin down`

6. If the cluster consists of only two nodes, disable cluster HA: `cluster ha modify -configured false`

7. Disable storage failover for the nodes in the HA pair from either node: `storage failover modify -node nodename -enabled false`

   You only need to disable storage failover once for the HA pair. When you disable storage failover for a node, storage failover is also disabled on the node's partner.

8. Log in to the node that you want to revert.
To revert a node, you must be logged in to the cluster through the node’s node management LIF.

9. Set the node’s target ONTAP software image to be the default image: `system image modify -node nodename -image target_image -isdefault true`

10. Verify that the target ONTAP software image is set as the default image for the node that you are reverting: `system image show`

The following example shows that version 9.1 is set as the default image on node0:

```
cluster1::*> system image show
     Is     Is                 Install
    Node   Image   Default Current Version    Date
        --- ------ ------- ------- --------   -------------------
    node0   image1  false   true    9.2        MM/DD/YYYY TIME
             image2  true    false   9.1        MM/DD/YYYY TIME
    node1   image1  true    true    9.2        MM/DD/YYYY TIME
             image2  false   false   9.1        MM/DD/YYYY TIME
4 entries were displayed.
```

11. If the cluster consists of only two nodes, verify that the node does not hold epsilon:
   a. Check whether the node currently holds epsilon: `cluster show -node nodename`

   The following example shows that the node holds epsilon:

   ```
   cluster1::*> cluster show -node node1
   Node: node1
       UUID: 026efc12-acla-11e0-80ed-0f7eba8fc313
       Epsilon: true
       Eligibility: true
       Health: true
   ```

   b. If the node holds epsilon, mark epsilon as false on the node so that epsilon can be transferred to the node’s partner: `cluster modify -node nodenameA -epsilon false`

   c. Transfer epsilon to the node’s partner by marking epsilon true on the partner node: `cluster modify -node nodenameB -epsilon true`

12. Verify that the node is ready for reversion: `system node revert-to -node nodename -check -only true -version 9.x`

   The check-only parameter identifies any preconditions that must be addressed before reverting, such as the following examples:

   - Disabling storage failover
- Disabling the Snapshot policy
- Deleting Snapshot copies that were created after upgrading to the later version of ONTAP

13. Verify that all of the preconditions have been addressed: `system node revert-to -node nodename -check-only true -version 9.x`

14. Revert the cluster configuration of the node: `system node revert-to -node nodename -version 9.x`

   The `-version` option refers to the target release. For example, if the software you installed and verified is ONTAP 9.1, the correct value of the `-version` option is 9.1.

   The cluster configuration is reverted, and then you are logged out of the clustershell.

15. Log back in to the clustershell, and then switch to the nodeshell: `run -node nodename`

   After logging on the clustershell again, it might take a few minutes before it is ready to accept the nodeshell command. So, if the command fails, wait a few minutes and try it again.

16. Revert the file system configuration of the node: `revert_to 9.x`

   This command verifies that the node’s file system configuration is ready to be reverted, and then reverts it. If any preconditions are identified, you must address them and then rerun the revert_to command.

   Using a system console to monitor the revert process displays greater details than seen in nodeshell.

   If AUTOBOOT is true, when the command finishes, the node will reboot to ONTAP.

   If AUTOBOOT is false, when the command finishes the LOADER prompt is displayed. Enter `yes` to revert; then use `boot_ontap` to manually reboot the node.

17. After the node has rebooted, confirm that the new software is running: `system node image show`

   In the following example, image1 is the new ONTAP version and is set as the current version on node0:

   ```
   cluster1::*> system node image show
   Is   Is                 Install
   Node Image Default Current Version    Date
   -------- ------- ------- ------- --------   -------------------
   node0   image1  true    true    X.X.X       MM/DD/YYYY TIME
   image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
   node1   image1  true    false   X.X.X      MM/DD/YYYY TIME
   image2  false   true    Y.Y.Y      MM/DD/YYYY TIME
   4 entries were displayed.
   ```

18. Verify that the revert status is complete for each node: `system node upgrade-revert show -node nodename`

20. If the cluster consists of only two nodes, reenable cluster HA: `cluster ha modify -configured true`

21. Reenable storage failover on both nodes if it was previously disabled: `storage failover modify -node nodename -enabled true`

22. Repeat [step-5] through [step-19] for each additional HA pair and both the clusters in MetroCluster Configuration.

**What should I do after reverting my cluster?**

**Verify cluster and storage health after downgrade or revert**

After you downgrade or revert a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum. You should also verify the status of your disks, aggregates, and volumes.

**Verify cluster health**

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster: `cluster show`

   ```
   cluster1::> cluster show
   Node          Health  Eligibility
   ----------------------- ------ -------
   node0         true     true
   node1         true     true
   ```

   If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:
   `set -privilege advanced`

   Enter `y` to continue.

3. Verify the configuration details for each RDB process.
   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.

   Note that each ring might have a different quorum master.

<table>
<thead>
<tr>
<th>To display this RDB process...</th>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management application</td>
<td><code>cluster ring show -unitname mgmt</code></td>
</tr>
<tr>
<td>Volume location database</td>
<td><code>cluster ring show -unitname vldb</code></td>
</tr>
</tbody>
</table>
To display this RDB process… Enter this command…

<table>
<thead>
<tr>
<th>Virtual-Interface manager</th>
<th>cluster ring show -unitname vifmgr</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN management daemon</td>
<td>cluster ring show -unitname bcomd</td>
</tr>
</tbody>
</table>

This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node  UnitName  Epoch  DB Epoch  DB Trnxs  Master  Online
     --------  --------  --------  --------  --------  --------  --------
node0 vldb      154      154      14847    node0     master
node1 vldb      154      154      14847    node0     secondary
node2 vldb      154      154      14847    node0     secondary
node3 vldb      154      154      14847    node0     secondary
4 entries were displayed.
```

4. Return to the admin privilege level: set -privilege admin

5. If you are operating in a SAN environment, verify that each node is in a SAN quorum: event log show -severity informational -message-name scsiblade.*

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show -severity informational -message-name scsiblade.*
Time             Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The...
```

Related information

System administration

Verify storage health

After you revert or downgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

1. Verify disk status:
To check for... | Do this...
---|---
**Broken disks** | a. Display any broken disks: `storage disk show -state broken`<br>b. Remove or replace any broken disks.

**Disks undergoing maintenance or reconstruction** | a. Display any disks in maintenance, pending, or reconstructing states: `storage disk show -state maintenance|pending|reconstructing`<br>b. Wait for the maintenance or reconstruction operation to finish before proceeding.

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates: `storage aggregate show -state !online`

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verify that all volumes are online by displaying any volumes that are *not* online: `volume show -state !online`

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

See the Knowledge Base article *Volume Showing WAFL Inconsistent* on how to address the inconsistent volumes.

**Related information**

*Disk and aggregate management*

**Enable automatic switchover for MetroCluster configurations**

This topic provides information regarding the additional tasks that you must perform after the reversion of MetroCluster configurations.

1. Enable automatic unplanned switchover: `metrocluster modify -auto-switchover-failure -domain auso-on-cluster-disaster`

2. Validate the MetroCluster configuration: `metrocluster check run`
Enable and revert LIFs to home ports after a revert

During a reboot, some LIFs might have been migrated to their assigned failover ports. After you revert a cluster, you must enable and revert any LIFs that are not on their home ports.

The network interface revert command reverts a LIF that is not currently on its home port back to its home port, provided that the home port is operational. A LIF’s home port is specified when the LIF is created; you can determine the home port for a LIF by using the network interface show command.

1. Display the status of all LIFs: `network interface show`

This example displays the status of all LIFs for a storage virtual machine (SVM).

```
cluster1::> network interface show -vserver vs0

<table>
<thead>
<tr>
<th>Logical</th>
<th>Status</th>
<th>Network</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vserver</td>
<td>Interface</td>
<td>Admin/Oper Address/Mask</td>
<td>Node</td>
</tr>
<tr>
<td>Home</td>
<td>-----------</td>
<td>-------------------</td>
<td>------------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical</th>
<th>Status</th>
<th>Network</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>data001</td>
<td>down/down</td>
<td>192.0.2.120/24</td>
<td>node0</td>
</tr>
<tr>
<td>true</td>
<td>data002</td>
<td>down/down</td>
<td>192.0.2.121/24</td>
<td>node0</td>
</tr>
<tr>
<td>true</td>
<td>data003</td>
<td>down/down</td>
<td>192.0.2.122/24</td>
<td>node0</td>
</tr>
<tr>
<td>true</td>
<td>data004</td>
<td>down/down</td>
<td>192.0.2.123/24</td>
<td>node0</td>
</tr>
<tr>
<td>true</td>
<td>data005</td>
<td>down/down</td>
<td>192.0.2.124/24</td>
<td>node0</td>
</tr>
<tr>
<td>false</td>
<td>data006</td>
<td>down/down</td>
<td>192.0.2.125/24</td>
<td>node0</td>
</tr>
<tr>
<td>false</td>
<td>data007</td>
<td>down/down</td>
<td>192.0.2.126/24</td>
<td>node0</td>
</tr>
<tr>
<td>false</td>
<td>data008</td>
<td>down/down</td>
<td>192.0.2.127/24</td>
<td>node0</td>
</tr>
</tbody>
</table>

8 entries were displayed.
```

If any LIFs appear with a Status Admin status of down or with an Is home status of false, continue with the next step.

2. Enable the data LIFs: `network interface modify { -role data } -status-admin up`
3. **Revert LIFs to their home ports**: `network interface revert *`

This command reverts all LIFs back to their home ports.

```
cluster1::> network interface revert *
8 entries were acted on.
```

4. **Verify that all LIFs are in their home ports**: `network interface show`

This example shows that all LIFs for SVM vs0 are on their home ports.

```
cluster1::> network interface show -vserver vs0

Current Is
Vserver Interface Admin/Oper Address/Mask Node Port
------- ---------- ------------------ --------------
true     data001  up/up    192.0.2.120/24 node0 e0e
true     data002  up/up    192.0.2.121/24 node0 e0f
true     data003  up/up    192.0.2.122/24 node0 e2a
true     data004  up/up    192.0.2.123/24 node0 e2b
true     data005  up/up    192.0.2.124/24 node1 e0e
true     data006  up/up    192.0.2.125/24 node1 e0f
true     data007  up/up    192.0.2.126/24 node1 e2a
true     data008  up/up    192.0.2.127/24 node1 e2b
```

8 entries were displayed.

**Enable Snapshot copy policies after reverting**

After reverting to an earlier version of ONTAP, you must enable Snapshot copy policies to
start creating Snapshot copies again.

You are reenabling the Snapshot schedules that you disabled before you reverted to an earlier version of ONTAP.

1. Enable Snapshot copy policies for all data SVMs:

   ```bash
   volume snapshot policy modify -vserver * -enabled true
   snapshot policy modify pg-rpo-hourly -enable true
   ```

2. For each node, enable the Snapshot copy policy of the root volume by using the `run-nodenodenamevol optionsroot_vol_namenosnap off` command.

   ```bash
   cluster1::> run -node node1 vol options vol0 nosnap off
   ```

**Verify client access (SMB and NFS)**

For the configured protocols, test access from SMB and NFS clients to verify that the cluster is accessible.

**Verify IPv6 firewall entries**

A reversion from any version of ONTAP 9 might result in missing default IPv6 firewall entries for some services in firewall policies. You need to verify that the required firewall entries have been restored to your system.

1. Verify that all firewall policies are correct by comparing them to the default policies: `system services firewall policy show`

   The following example shows the default policies:
cluster1::*> system services firewall policy show

<table>
<thead>
<tr>
<th>Policy</th>
<th>Service</th>
<th>Action</th>
<th>IP-List</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster</td>
<td>dns</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>http</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>https</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>ndmp</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>ntp</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>rsh</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>snmp</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>ssh</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>telnet</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>data</td>
<td>dns</td>
<td>allow</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>http</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>https</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>ndmp</td>
<td>allow</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>ntp</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>rsh</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
</tbody>
</table>

2. Manually add any missing default IPv6 firewall entries by creating a new firewall policy: system services firewall policy create

   cluster1::*> system services firewall policy create -policy newIPv6
               -service ssh -action allow -ip-list ::/0

3. Apply the new policy to the LIF to allow access to a network service: network interface modify

   cluster1::*> network interface modify -vserver VS1 -lif LIF1
               -firewall-policy newIPv6

Revert password hash function to the supported encryption type

If you reverted from ONTAP 9.1 or ONTAP 9.0 to ONTAP 8.3.x, SHA-2 account users can no longer be authenticated with their passwords. Passwords must be reset to use the MDS encryption type.

1. Set a temporary password for each SHA-2 user account that you identified prior to reverting: security login password -username user_name -vserver vserver_name
2. Communicate the temporary password to the affected users and have them log in through a console or SSH session to change their passwords as prompted by the system.

**Considerations for whether to manually update the SP firmware**

If the SP automatic update functionality is enabled (the default), downgrading or reverting to ONTAP 8.3.x does not require a manual SP firmware update. The SP firmware is automatically updated to the newest compatible version that is supported by the ONTAP version you reverted or downgraded to.

If the SP automatic update functionality is disabled (not recommended), after the ONTAP revert or downgrade process is complete, you must manually update the SP firmware to a version that is supported for the ONTAP version you reverted or downgraded to.

**NetApp BIOS/ONTAP Support Matrix**

**NetApp Downloads: System Firmware and Diagnostics**

**Change in user accounts that can access the Service Processor**

If you created user accounts on ONTAP 9.8 or earlier, upgraded to ONTAP 9.9.1 or later (when the `role` parameter is changed to `admin`), and then reverted back to ONTAP 9.8 or earlier, the `role` parameter is restored to its original value. You should nonetheless verify that the modified values are acceptable.

During revert, if the role for an SP user has been deleted, the "rbac.spuser.role.notfound" EMS message will be logged.

For more information, see Accounts that can access the SP.