



Upgrade ONTAP

ONTAP 9

NetApp
March 08, 2024

This PDF was generated from <https://docs.netapp.com/us-en/ontap/upgrade/index.html> on March 08, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Upgrade ONTAP 1
 - ONTAP upgrade overview 1
 - When should I upgrade ONTAP?..... 1
 - Execute ONTAP automated pre-upgrade checks before a planned upgrade 2
 - Prepare for an ONTAP upgrade..... 14
 - Download the ONTAP software image..... 64
 - ONTAP upgrade methods 65
 - What to do after an ONTAP upgrade 118

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.

Example 1. Steps

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 You should have already downloaded the image to the local client.	<ol style="list-style-type: none">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.
Add a new software image from an HTTP or FTP server	<ol style="list-style-type: none">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.

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  
http://www.example.com/software/9.13.1/image.tgz
```

```
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:

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



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	OK	N/A
Aggregate online status and parity check	OK	N/A
Aggregate plex resync status check	OK	N/A
Application Provisioning Cleanup	OK	N/A
Autoboot Bootargs Status	OK	N/A
Backend	OK	N/A
...		
Volume Conversion	OK	N/A
In Progress Check		
Volume move progress status check	OK	N/A
Volume online status check	OK	N/A
iSCSI target portal groups status check	OK	N/A
Overall Status	Warning	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
```

Update Phase	Status	Estimated Duration	Elapsed Duration
Pre-update checks	in-progress	00:10:00	00:00:42

Details:

Pre-update Check	Status	Error-Action
-----	-----	-----
-----	-----	-----

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

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

Details:

Pre-update Check	Status	Error-Action
-----	-----	-----
AMPQ Router and Broker Config Cleanup	OK	N/A
Aggregate online status and parity check	OK	N/A
Aggregate plex resync status check	OK	N/A
Application Provisioning Cleanup	OK	N/A
Autoboot Bootargs Status	OK	N/A
Backend Configuration Status	OK	N/A
Boot Menu Status	Warning	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.
Broadcast Domain availability and uniqueness for HA pair status	OK	N/A
CIFS compatibility status check	OK	N/A
CLAM quorum online status check	OK	N/A
CPU Utilization Status	OK	N/A
Capacity licenses install status check	OK	N/A
Check For SP/BMC Connectivity To Nodes	OK	N/A

Check LDAP fastbind users using unsecure connection.	OK	N/A
Check for unsecure kex algorithm configurations.	OK	N/A
Check for unsecure mac configurations.	OK	N/A
Cloud keymanager connectivity check	OK	N/A
Cluster health and eligibility status	OK	N/A
Cluster quorum status check	OK	N/A
Cluster/management switch check	OK	N/A
Compatible New Image Check	OK	N/A
Current system version check if it is susceptible to possible outage during NDU	OK	N/A
Data ONTAP Version and Previous Upgrade Status	OK	N/A
Data aggregates HA policy check	OK	N/A
Disk status check for failed, broken or non-compatibility	OK	N/A
Duplicate Initiator Check	OK	N/A
Encryption key migration status check	OK	N/A
External key-manager with legacy KMIP client check	OK	N/A
External keymanager key server status check	OK	N/A
Fabricpool Object Store Availability	OK	N/A
High Availability	OK	N/A

configuration		
status check		
Infinite Volume	OK	N/A
availability check		
LIF failover	OK	N/A
capability status		
check		
LIF health check	OK	N/A
LIF load balancing	OK	N/A
status check		
LIFs is on home	OK	N/A
node status		
Logically over	OK	N/A
allocated DP		
volumes check		
MetroCluster	OK	N/A
configuration		
status check for		
compatibility		
Minimum number of	OK	N/A
aggregate disks		
check		
NAE Aggregate and	OK	N/A
NVE Volume		
Encryption Check		
NDMP sessions check	OK	N/A
NFS mounts status	Warning	Warning: This cluster is serving
NFS		
check		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
Name Service	OK	N/A
Configuration DNS		
Check		
Name Service	OK	N/A

Configuration LDAP

Check

Node to SP/BMC connectivity check	OK	N/A
OKM/KMIP enabled systems - Missing keys check	OK	N/A
ONTAP API to REST transition warning data last 30 days approaching automation REST	Warning	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 tools from ONTAP API to ONTAP API. For more details, refer to CPC-00410 - End of availability: ONTAPI
		https://mysupport.netapp.com/info/communications/ECMLP2880232.html
ONTAP Image Capability Status	OK	N/A
OpenSSL 3.0.x upgrade validation check	OK	N/A
Openssh 7.2 upgrade validation check	OK	N/A
Platform Health Monitor check	OK	N/A
Pre-Update Configuration Verification	OK	N/A
RDB Replica Health Check	OK	N/A
Replicated database schema consistency check	OK	N/A
Running Jobs Status	OK	N/A
SAN LIF association status check	OK	N/A

SAN compatibility for manual configurability check	OK	N/A
SAN kernel agent status check	OK	N/A
Secure Purge operation Check	OK	N/A
Shelves and Sensors check	OK	N/A
SnapLock Version Check	OK	N/A
SnapMirror Synchronous relationship status check	OK	N/A
SnapMirror compatibility status check	OK	N/A
Supported platform check	OK	N/A
Target ONTAP release support for FiberBridge 6500N check	OK	N/A
Upgrade Version Compatibility Status	OK	N/A
Verify all bgp peer-groups are in the up state	OK	N/A
Verify if a cluster management LIF exists	OK	N/A
Verify that e0M is home to no LIFs with high speed services.	OK	N/A
Volume Conversion In Progress Check	OK	N/A
Volume move progress status check	OK	N/A
Volume online status check	OK	N/A
iSCSI target portal groups status check	OK	N/A

Prepare for an ONTAP upgrade

Prepare for an ONTAP software 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.

If your current ONTAP release is...	And your target ONTAP release is...	Your automated or manual upgrade path is...
9.13.1	9.14.1	direct
9.12.1	9.14.1	direct
	9.13.1	direct
9.11.1	9.14.1	direct
	9.13.1	direct
	9.12.1	direct
9.10.1	9.14.1	direct
	9.13.1	direct
	9.12.1	direct
	9.11.1	direct

From ONTAP 9.9.1

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

If your current ONTAP release is...	And your target ONTAP release is...	Your automated or manual upgrade path is...
9.9.1	9.14.1	multi-stage -9.9.1→9.13.1 -9.13.1→9.14.1
	9.13.1	direct
	9.12.1	direct
	9.11.1	direct
	9.10.1	direct

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.

If your current ONTAP release is...	And your target ONTAP release is...	Your automated or and manual upgrade path is...
9.8	9.14.1	multi-stage -9.8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-stage -9.8 → 9.12.1 -9.12.1 → 9.13.1
	9.12.1	direct
	9.11.1	direct
	9.10.1	direct
	9.9.1	direct

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

If your current ONTAP release is...	And your target ONTAP release is...	Your automated upgrade path is...
9.7	9.14.1	multi-stage -9.7 → 9.8 -9.8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-stage -9.7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1	multi-stage -9.7 → 9.8 -9.8 → 9.12.1
	9.11.1	direct multi-hop (requires images for 9.8 and 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	direct
	9.8	direct

Manual paths

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.7	9.14.1	multi-stage -9.7 → 9.8 -9.8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-stage -9.7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1	multi-stage - 9.7 → 9.8 - 9.8 → 9.12.1
	9.11.1	multi-stage - 9.7 → 9.8 - 9.8 → 9.11.1
	9.10.1	multi-stage - 9.7 → 9.8 - 9.8 → 9.10.1
	9.9.1	direct
	9.8	direct

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.

Automated paths

If your current ONTAP release is...	And your target ONTAP release is...	Your automated upgrade path is...
9.6	9.14.1	multi-stage -9.6 → 9.8 -9.8 → 9.12.1 -9.12.1 → 9.14.1
	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
	9.8	direct
	9.7	direct

Manual paths

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.6	9.14.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.12.1 - 9.12.1 → 9.14.1
	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	multi-stage - 9.6 → 9.8 - 9.8 → 9.10.1
	9.9.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.9.1
	9.8	direct
	9.7	direct

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

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

Manual upgrade paths

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.5	9.14.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 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 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.5 → 9.7 - 9.7 → 9.8
	9.7	direct
	9.6	direct

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

If your current ONTAP release is...	And your target ONTAP release is...	Your automated upgrade path is...
9.4	9.14.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)
	9.8	multi-stage - 9.4 → 9.5 - 9.5 → 9.8 (direct multi-hop, requires images for 9.7 and 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
	9.5	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your automated upgrade path is...
9.3	9.14.1	multi-stage - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) - 9.7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) - 9.7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) - 9.7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) - 9.7 → 9.10.1 (direct multi-hop, requires images for 9.8 and 9.10.1)
	9.9.1	multi-stage - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) - 9.7 → 9.9.1
	9.8	multi-stage - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) - 9.7 → 9.8
	9.7	direct multi-hop (requires images for 9.5 and 9.7)
	9.6	multi-stage - 9.3 → 9.5 - 9.5 → 9.6
	9.5	direct
	9.4	not available

If your current ONTAP release is...	And your target ONTAP release is...	Your automated upgrade path is...
9.2		

	9.7	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7
If your current ONTAP release is...	And your target ONTAP release is...	Your auto-upgrade path is...
	9.6	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.3 → 9.5 - 9.5 → 9.6
	9.4	not available
	9.3	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your automated upgrade path is...
9.1		

If your current ONTAP release is...	9.7	multi-stage - 9.1 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)
	9.6	multi-stage - 9.1 → 9.3 - 9.3 → 9.6 (direct multi-hop, requires images for 9.5 and 9.6)
	9.5	multi-stage - 9.1 → 9.3 - 9.3 → 9.5
	9.4	not available
	9.3	direct
	9.2	not available

If your current ONTAP release is...	And your target ONTAP release is...	Your automated upgrade path is...
9.0		

If your current ONTAP release is...	And your target ONTAP release is...	- 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) - 9.7 → 9.9.1
		Your automated upgrade path is...
	9.8	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) - 9.7 → 9.8
	9.7	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)
	9.6	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5
	9.4	not available
	9.3	multi-stage - 9.0 → 9.1 - 9.1 → 9.3
	9.2	not available
	9.1	direct

Manual upgrade paths

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.4	9.14.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.12.1 → 9.14.1
	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
	9.5	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
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 - 9.12.1 → 9.14.1
	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
	9.5	direct
	9.4	not available

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.2		

	9.7	multi-stage - 9.2 → 9.3 - 9.5 → 9.7
If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
	9.6	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.2 → 9.3 - 9.3 → 9.5
	9.4	not available
	9.3	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.1		

	9.7	multi-stage - 9.1 → 9.3 - 9.3 → 9.5
If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
	9.6	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.1 → 9.3 - 9.3 → 9.5
	9.4	not available
	9.3	direct
	9.2	not available

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.0		

		- 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.7 → 9.9.1
If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
	9.8	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
	9.7	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5
	9.4	not available
	9.3	multi-stage - 9.0 → 9.1 - 9.1 → 9.3
	9.2	not available
	9.1	direct

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:

If your ONTAP version is...	Use this command
9.6 or later	<code>network interface show -service-policy *data* -failover</code>
9.5 or earlier	<code>network interface show -role data -failover</code>

This example shows the default failover configuration for a two-node cluster with two data LIFs:

```
cluster1::> network interface show -role data -failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
vs0	lif0	node0:e0b	nextavail	system-
defined		Failover Targets: node0:e0b, node0:e0c, node0:e0d, node0:e0e, node0:e0f, node1:e0b, node1:e0c, node1:e0d, node1:e0e, node1:e0f		
vs1	lif1	node1:e0b	nextavail	system-
defined		Failover Targets: node1:e0b, node1:e0c, node1:e0d, node1:e0e, node1:e0f, node0:e0b, node0:e0c, node0:e0d, node0:e0e, node0:e0f		

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.

Before you upgrade ONTAP, ask yourself...	If your answer is yes, then do this...
Is my cluster currently in a mixed version state?	Check mixed version requirements
Do I have a MetroCluster configuration?	Review specific upgrade requirements for MetroCluster configurations
Do I have a SAN configuration?	Verify the SAN host configuration
Does my cluster have SnapMirror relationships defined?	Verify compatibility of ONTAP versions for SnapMirror relationships
Do I have DP-type SnapMirror relationships defined, and am I upgrading to ONTAP 9.12.1 or later?	Convert existing DP-type relationships to XDP
Am I using NetApp Storage Encryption with external key management servers?	Delete any existing key management server connections
Do I have netgroups loaded into SVMs?	Verify that the netgroup file is present on each node
Do I have LDAP clients using SSLv3?	Configure LDAP clients to use TLS
Am I using session-oriented protocols?	Review considerations for session-oriented protocols

Before you upgrade ONTAP, ask yourself...	If your answer is yes, then do this...
Is SSL FIPS mode enabled on a cluster where administrator accounts authenticate with an SSH public key?	Verify SSH host key algorithm support

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.

If the lowest version of ONTAP running in the mixed version cluster is:	Then you can remain in a mixed version state for a maximum of
ONTAP 9.8 or higher	90 days
ONTAP 9.7 or lower	7 days

- 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 met 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.

For...	Enter...
iSCSI	<pre>iscsi initiator show -fields igroup,initiator-name,tpgroup</pre>
FC	<pre>fcp initiator show -fields igroup,wwpn,lif</pre>

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

ONTAP version ...	Interoperates with these previous ONTAP versions...																	
	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5	9.4	9.3
9.14.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No
9.14.0*	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	No	No	No	No
9.13.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
9.13.0*	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	No	No	No	No
9.12.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No
9.12.0*	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes	No	No	No	No
9.11.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
9.11.0*	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	No	No	No
9.10.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.10.0*	Yes	No	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No
9.9.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.9.0*	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.8	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
9.7	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
9.6	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
9.5	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9.4	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
9.3	No	No	No	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes

SnapMirror Synchronous relationships



SnapMirror Synchronous is not supported for ONTAP cloud instances.

ONTAP version ...	Interoperates with these previous ONTAP versions...									
	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.14.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
9.13.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.12.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.11.1	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No
9.10.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
9.9.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.8	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No
9.7	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes
9.6	No	No	No	No	No	No	Yes	Yes	Yes	Yes
9.5	No	No	No	No	No	No	No	Yes	Yes	Yes

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).

Source	Destination																	
	9.3	9.4	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1
9.3	DR/Migration	Migration	Migration	Migration	Migration													

9.4		DR/ Migr atio n	Migr atio n	Migr atio n	Migr atio n	Migr atio n											
9.5			DR/ Migr atio n	Migr atio n	Migr atio n	Migr atio n	Migr atio n										
9.6				DR/ Migr atio n	Migr atio n	Migr atio n	Migr atio n	Migr atio n									
9.7					DR/ Migr atio n	Migr atio n	Migr atio n	Migr atio n	Migr atio n								
9.8						DR/ Migr atio n	Migr atio n	Migr atio n	Migr atio n	Migr atio n							
9.9. 0*							DR/ Migr atio n	Migr atio n	Migr atio n	Migr atio n	Migr atio n						
9.9. 1								DR/ Migr atio n	Migr atio n	Migr atio n	Migr atio n	Migr atio n					
9.10 .0*									DR/ Migr atio n	Migr atio n	Migr atio n	Migr atio n	Migr atio n				
9.10 .1										DR/ Migr atio n	Migr atio n	Migr atio n	Migr atio n	Migr atio n			
9.11 .0*											DR/ Migr atio n	Migr atio n	Migr atio n	Migr atio n	Migr atio n		
9.11 .1												DR/ Migr atio n	Migr atio n	Migr atio n	Migr atio n	Migr atio n	

9.12.0*													DR/Migration	Migration	Migration	Migration	Migration	
9.12.1													DR/Migration	Migration	Migration	Migration	Migration	
9.13.0*														DR/Migration	Migration	Migration	Migration	
9.13.1															DR/Migration	Migration	Migration	
9.14.0*																DR/Migration	Migration	
9.14.1																	DR/Migration	

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.

Source	Destination											
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3	9.2	9.1	9
9.11.1	Yes	No	No	No	No	No	No	No	No	No	No	No
9.10.1	Yes	Yes	No	No	No	No	No	No	No	No	No	No
9.9.1	Yes	Yes	Yes	No	No	No	No	No	No	No	No	No
9.8	No	Yes	Yes	Yes	No	No	No	No	No	No	No	No
9.7	No	No	Yes	Yes	Yes	No	No	No	No	No	No	No
9.6	No	No	No	Yes	Yes	Yes	No	No	No	No	No	No

9.5	No	No	No	No	Yes	Yes	Yes	No	No	No	No	No
9.4	No	No	No	No	No	Yes	Yes	Yes	No	No	No	No
9.3	No	No	No	No	No	No	Yes	Yes	Yes	No	No	No
9.2	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No
9.1	No	No	No	No	No	No	No	No	Yes	Yes	Yes	No
9	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes



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: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
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%
-----
svm1 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
```

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  
-relationship-info-only true
```

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):

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

4. Verify that assigning the FIPS key to all disks is complete:

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

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

```
storage encryption disk show
```

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:

```
vserver services netgroup status
```

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.

ONTAP release	Key types supported in FIPS mode	Key types supported in non-FIPS mode
9.11.1 and later	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa



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.

If you are running...	You can download the image to this location...
ONTAP 9.6 and later	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 on 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 upgrade.

Recommended ONTAP upgrade methods based on configuration

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

Configuration	ONTAP version	Number of nodes	Recommended upgrade method
Standard	9.0 or later	2 or more	<ul style="list-style-type: none"> • Automated nondisruptive using System Manager • Automated nondisruptive using the CLI
Standard	9.0 or later	Single	Automated disruptive
MetroCluster	9.3 or later	8	<ul style="list-style-type: none"> • Automated nondisruptive using the CLI • Manual nondisruptive for 4 or 8 node MetroCluster using the CLI
MetroCluster	9.3 or later	2,4	<ul style="list-style-type: none"> • 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.



Modifying the setting of the `storage failover modify-auto-giveback` command option before the start of an automatic nondisruptive upgrade (ANDU) has no impact on the upgrade process. The ANDU process ignores any preset value to this option during the takeover/giveback required for the update. For example, setting `-autogiveback` to false prior to beginning ANDU does not interrupt the automatic upgrade before giveback.

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:



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 You should have already downloaded the image to the local client.	<ol style="list-style-type: none">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.
Add a new software image from an HTTP or FTP server	<ol style="list-style-type: none">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  
http://www.example.com/software/9.13.1/image.tgz
```

```
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:

```
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
```

- d. Execute the automated pre-upgrade checks:

```
cluster 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:

```
cluster 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:

```
cluster 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
```

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

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:

```
metrocluster 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:

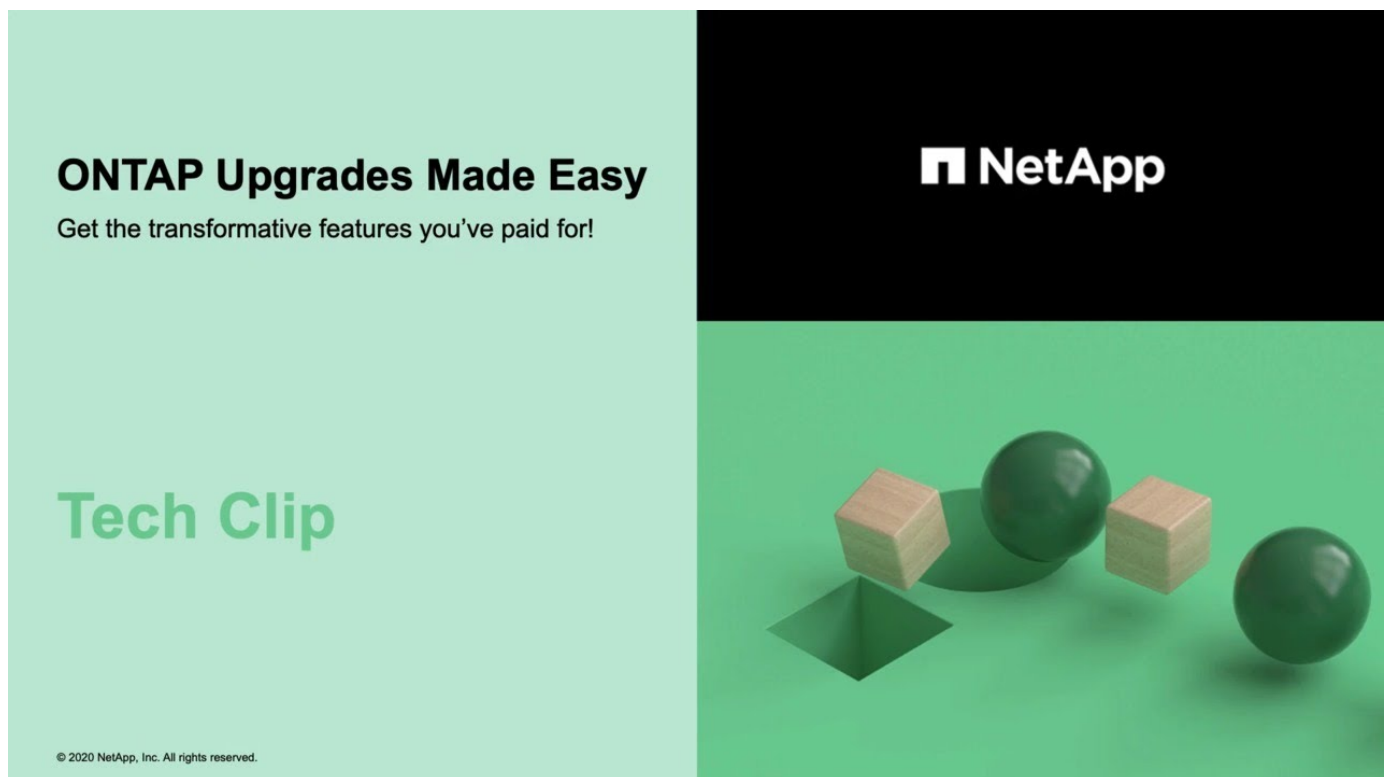
```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster
```

- 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:

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

2. Download the target ONTAP software package:

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

```
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:

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

```
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:

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

```
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:

If you are running...	Then...
ONTAP 9.8 or later	Click Cluster > Overview
ONTAP 9.7, 9.6, or 9.5	Click Configuration > Cluster > Update .
ONTAP 9.4 or earlier	<ul style="list-style-type: none">• 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.

If you want to...	Then...
Resume the automated upgrade	Click Resume .
Cancel the automated upgrade and continue manually	Click Cancel .

CLI

1. View the upgrade error:

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

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

If you want to...	Enter the following command...
Resume the automated upgrade	<pre>cluster image resume-update</pre>
Cancel the automated upgrade and continue manually	<pre>cluster image cancel-update</pre>

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.

If you have the following configuration...	Use this command...
<ul style="list-style-type: none">• Non-MetroCluster• 2-node MetroCluster	<div><pre>system node image update -node * -package _location_ -replace -package true -setdefault true -background true</pre></div> <p><i>location</i> can be a web server or a local folder, depending on the ONTAP version. See the <code>system node image update</code> man page for details.</p> <p>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 <code>-background</code> parameter.</p>
<ul style="list-style-type: none">• 4-node MetroCluster• 8-node MetroCluster configuration	<div><pre>system node image update -node * -package location -replace -package true -background true -setdefault false</pre></div> <p>You must issue this command on both clusters.</p> <p>This command uses an extended query to change the target software image, which is installed as the alternate image on each node.</p>

- 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:

```
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.
```

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:

```
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:

```
set -privilege advanced
```

The advanced prompt (*>) appears.

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

```
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:

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

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

```
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
```

Node	Image	Is Default	Is Current	Version	Install Date

node0					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME

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
```

```
cluster1::> 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.

```
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:

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

10. Verify 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 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.

```
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
```

Node	Partner	Takeover Possible	State Description
node0	node1	-	Waiting for giveback (HA mailboxes)
node1	node0	false	In takeover

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
	e1a	Cluster	Cluster	up	9000	auto/10000
	e1b	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
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
vs0					
	data001	up/up	192.0.2.120/24	node0	e0a
true					
	data002	up/up	192.0.2.121/24	node0	e0b
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
```

Node	Image	Is Default	Is Current	Version	Install 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	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

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.

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node0	node1	-	In takeover
node1	node0	false	Waiting for giveback (HA mailboxes)

2 entries were displayed.

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:

- Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
- If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
- 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 :

```
set -privilege advanced
```

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

```
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:

```
set -privilege admin
```

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

```
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:

```
cluster1::> network port show -node node1
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	

node1						
	e0M	Default	-	up	1500	auto/100
	e0a	Default	-	up	1500	auto/1000
	e0b	Default	-	up	1500	auto/1000
	e1a	Cluster	Cluster	up	9000	auto/10000
	e1b	Cluster	Cluster	up	9000	auto/10000
5 entries were displayed.						

19. 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.
```

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
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
vs0					
	data001	up/up	192.0.2.120/24	node1	e0a
true					
	data002	up/up	192.0.2.121/24	node1	e0b
true					
	data003	up/up	192.0.2.122/24	node1	e0b
true					
	data004	up/up	192.0.2.123/24	node1	e0a
true					

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
```

Node	Image	Is Default	Is Current	Version	Install 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
```

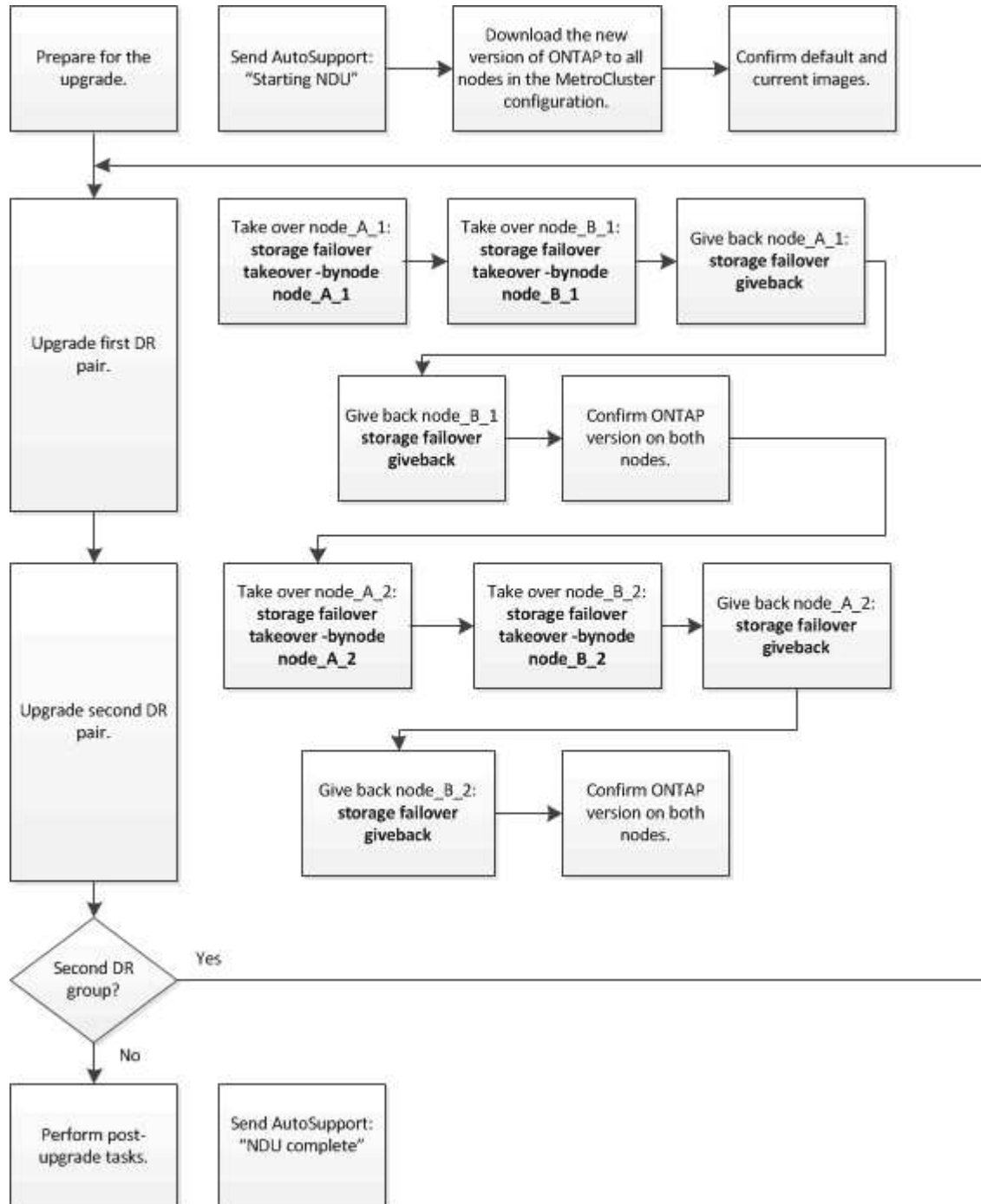
27. Upgrade any additional HA pairs.

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:

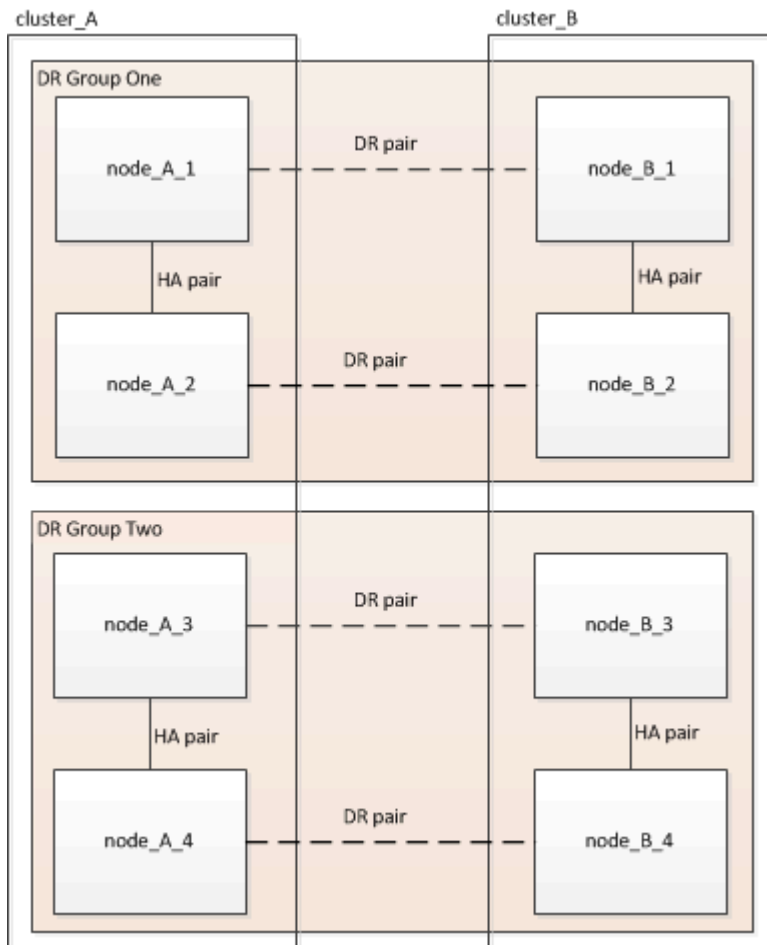
- Four-node MetroCluster FC or IP configurations running ONTAP 9.2 or earlier
- Eight-node MetroCluster FC configurations, regardless of ONTAP version
- If you have a two-node MetroCluster configuration, do not use this procedure.
- The following tasks refer to the old and new versions of ONTAP.
 - When 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:



You upgrade one DR group at a time.

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.

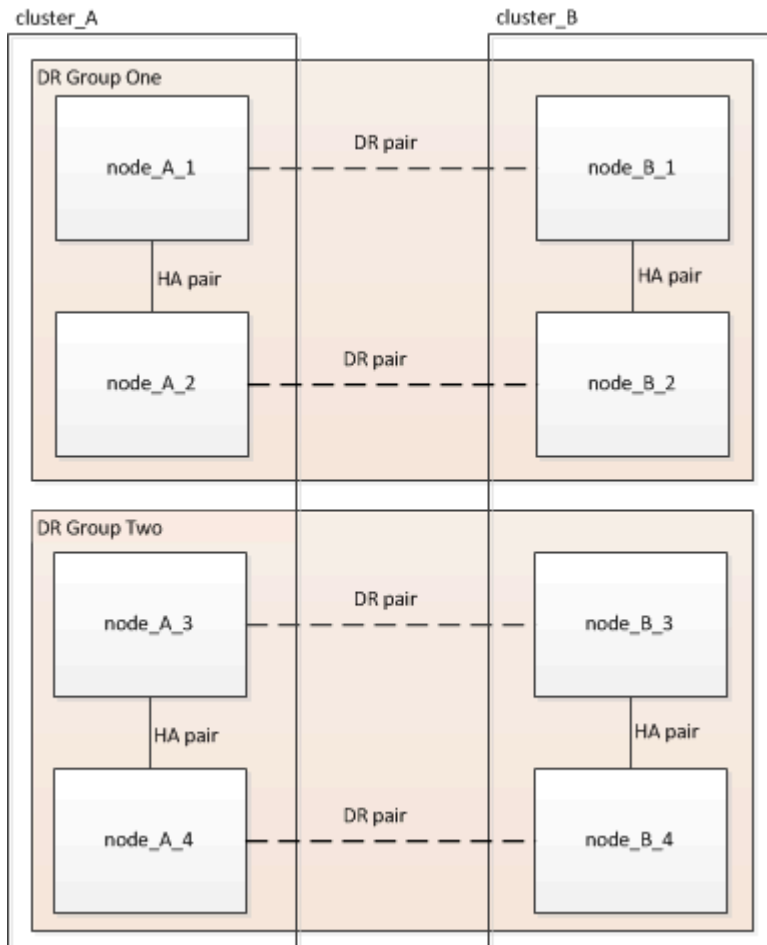
Preparing to upgrade a MetroCluster DR group

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
```

```
cluster_A::> metrocluster node show -fields dr-partner
(metrocluster node show)
dr-group-id cluster      node      dr-partner
-----
1          cluster_A    node_A_1  node_B_1
1          cluster_A    node_A_2  node_B_2
1          cluster_B    node_B_1  node_A_1
1          cluster_B    node_B_2  node_A_2
4 entries were displayed.

cluster_A::>
```

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
```

Node	Image	Is Default	Is Current	Version	Install 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
```

Node	Image	Is Default	Is Current	Version	Install Date

node_B_1					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME
node_B_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_B::>
```

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:

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install 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.

- 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
```

Node	Image	Is Default	Is Current	Version	Install Date

node_A_1	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/YY/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
```

Node	Partner	Takeover 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:

```
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:

```
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
```

Node	Partner	Takeover 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:

```
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:
- Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
 - If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
 - 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 be the default and current version on node_A_1:

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date

node_A_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	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

4 entries were displayed.

```
cluster_A::>
```

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
```

Node	Image	Is Default	Is Current	Version	Install Date

node_B_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_B_2					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

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
```

Node	Partner	Takeover Possible	State Description
node_A_1	node_A_2	false	In takeover
node_A_2	node_A_1	-	Waiting for giveback (HA mailboxes)

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):

If you are upgrading from...	Enter this command...
ONTAP 9.2 or ONTAP 9.1	<pre>storage failover takeover -ofnode node_B_2</pre>
ONTAP 9.0 or Data ONTAP 8.3.x	<pre>storage failover takeover -ofnode node_B_2 -option allow- version-mismatch</pre> <div><p>The <code>allow-version-mismatch</code> option is not required for upgrades from ONTAP 9.0 to ONTAP 9.1 or for any patch upgrades.</p></div>

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

Node           Partner           Takeover
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 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
```

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

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
```

Node	Image	Is Default	Is Current	Version	Install Date
node_B_1	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_B_2	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME

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
```

Node	Image	Is Default	Is Current	Version	Install Date

node_B_1					
	OldImage	false	true	X.X.X	MM/DD/YYYY TIME
	NewImage	true	false	Y.Y.Y	MM/DD/YYYY TIME

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 vservers 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
```

```
cluster_A::> metrocluster heal -phase root-aggregates  
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

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 vservers 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:

```
set -privilege advanced
```

d. Simulate the switchover operation:

```
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:

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

- 4. Perform either one of the following steps:

If the cluster consists of...	Do this...
One node	Continue to the next step.

If the cluster consists of...	Do this...
Two nodes	<p>a. Disable cluster high availability:</p> <pre>cluster ha modify -configured false</pre> <p>Enter y to continue when prompted.</p> <p>b. Disable storage failover for the HA pair:</p> <pre>storage failover modify -node * -enabled false</pre>
More than two nodes	<p>Disable storage failover for each HA pair in the cluster:</p> <pre>storage failover modify -node * -enabled false</pre>

5. Reboot a node in the cluster:

```
system node reboot -node nodename -ignore-quorum-warnings
```



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:

```
cluster1::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install 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.

8. Verify that the upgrade is completed successfully:

- a. Set the privilege level to advanced:

```
set -privilege advanced
```

- b. Verify that the upgrade status is complete for each node:

```
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:

```
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:

```
storage failover modify -node * -enabled true
```

11. If the cluster consists of only two nodes, enable cluster high availability:

```
cluster ha modify -configured true
```

What to do after an ONTAP upgrade

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.

4. [Update the Disk Qualification Package \(DQP\).](#)

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.

To display this RDB process...	Enter this command...
Management application	cluster ring show -unitname mgmt
Volume location database	cluster ring show -unitname vl原因db
Virtual-Interface manager	cluster ring show -unitname vifmgr
SAN management daemon	cluster ring show -unitname bcomd

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. 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	Node	Status	Status
cluster1-01	cluster1-01	in-quorum	true
cluster1-02	cluster1-02	in-quorum	true

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
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0						
	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	true

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.

Ask yourself...	If your answer is yes, then do this...
Did I upgrade from ONTAP 9.7 or earlier to ONTAP 9.8 or later?	Verify your network configuration Remove the EMS LIF service from network service policies that do not provide reachability to the EMS destination
Is my cluster in a MetroCluster configuration?	Verify your networking and storage status
Do I have a SAN configuration?	Verify your SAN configuration
Did I upgrade from ONTAP 9.3 or earlier, and am using NetApp Storage Encryption?	Reconfigure KMIP server connections
Do I have load-sharing mirrors?	Relocate moved load-sharing mirror source volumes
Does my cluster have defined SnapMirror relationships?	Resume SnapMirror operations
Do I have user accounts for Service Processor (SP) access that were created prior to ONTAP 9.9.1?	Verify the change in accounts that can access the Service Processor

Verify your networking configuration after an ONTAP upgrade from ONTAP 9.7x or earlier

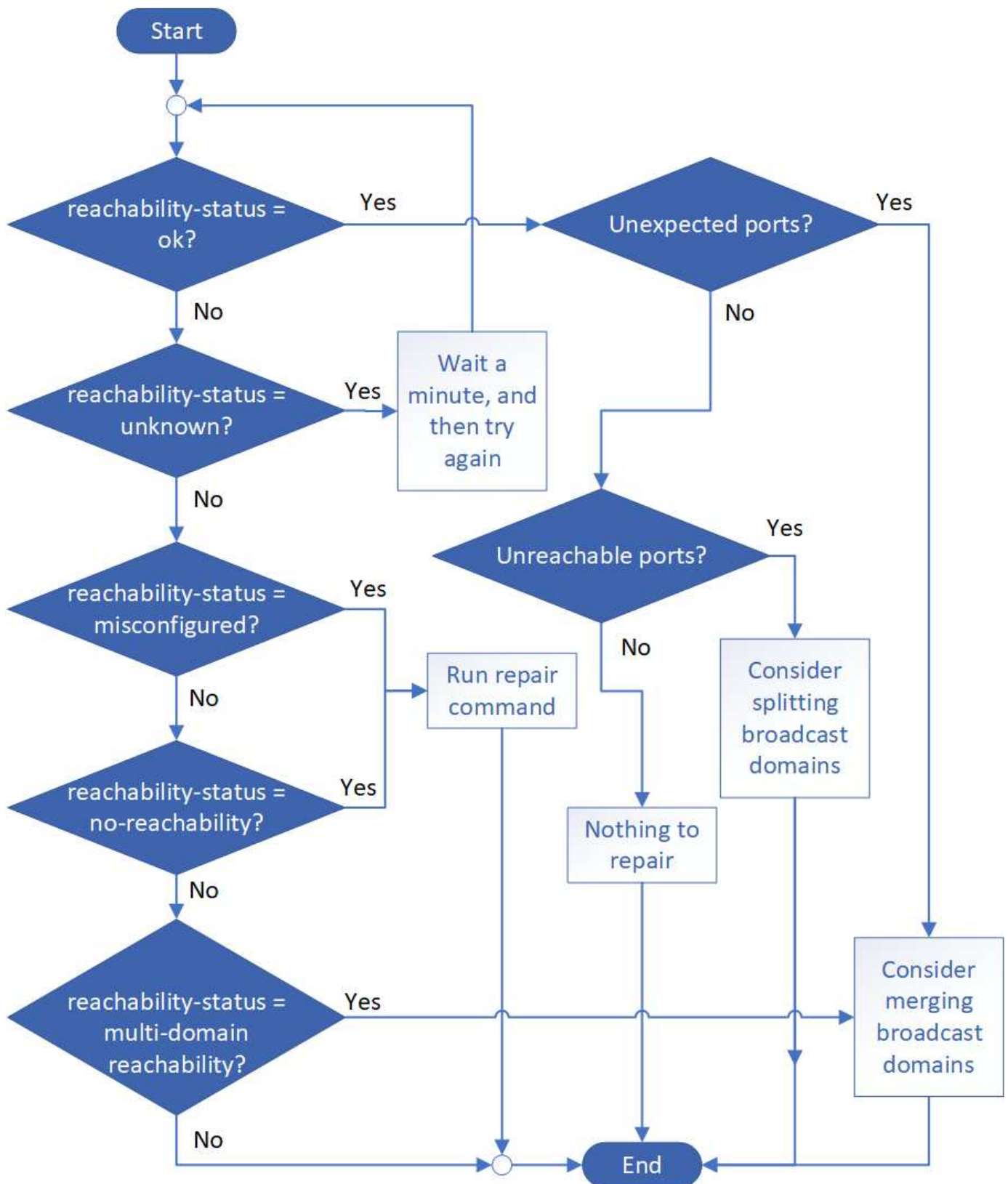
After you upgrade from ONTAP 9.7x or earlier to ONTAP 9.8 or later, you should verify your network configuration. After the upgrade, ONTAP automatically monitors layer 2 reachability.

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.



reachability-status	Description
---------------------	-------------

ok	<p>The port has layer 2 reachability to its assigned broadcast domain.</p> <p>If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see Merge broadcast domains.</p> <p>If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see Split broadcast domains.</p> <p>If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.</p>
misconfigured-reachability	<p>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.</p> <p>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:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see Repair port reachability.</p>
no-reachability	<p>The port does not have layer 2 reachability to any existing broadcast domain.</p> <p>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:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see Repair port reachability.</p>
multi-domain-reachability	<p>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.</p> <p>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.</p> <p>For more information, see Merge broadcast domains or Repair port reachability.</p>
unknown	<p>If the reachability-status is "unknown", then wait a few minutes and try the command again.</p>

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 policies. This allows EMS messages to be sent from any of the LIFs associated with any of the service policies. 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 policies that do not provide reachability to the destination.

Steps

1. Identify the LIFs and associated network service policies through which EMS messages can be sent:

```
network interface show -fields service-policy -services management-ems
```

vserver	lif	service-policy
cluster-1	cluster_mgmt	
		default-management
cluster-1	node1-mgmt	
		default-management
cluster-1	node2-mgmt	
		default-management
cluster-1	inter_cluster	
		default-intercluster

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 policies 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

```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
Cluster					
	cluster1-a1_clus1	up/up	192.0.2.1/24	cluster1-01	e2a
true					
	cluster1-a1_clus2	up/up	192.0.2.2/24	cluster1-01	e2b
true					
cluster1-01					
	clus_mgmt	up/up	198.51.100.1/24	cluster1-01	e3a
true					
	cluster1-a1_inet4_intercluster1	up/up	198.51.100.2/24	cluster1-01	e3c
true					
	...				

```

27 entries were displayed.

```

2. Verify the state of the aggregates:

```
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:

```

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:

```
cluster1::> 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)
Vserver   Volume      Aggregate   State   Type   Size
Available Used%
-----
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.

For...	Enter...
iSCSI	<pre>iscsi initiator show -fields igroup,initiator-name,tpgroup</pre>
FC	<pre>fcp initiator show -fields igroup,wwpn,lif</pre>

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:

```
storage encryption disk modify -disk disk_id -fips-key-id  
fips_authentication_key_id
```

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
```

Source	Destination	Mirror	Relationship	Total	Last	Path	Type	Path	State	Status	Progress	Healthy
cluster1-vs1:dp_src1	DP	cluster1-vs2:dp_dst1	Snapmirrored									
			Idle	-							true	-
cluster1-vs1:xdp_src1	XDP	cluster1-vs2:xdp_dst1	Snapmirrored									
			Idle	-							true	-
cluster1://cluster1-vs1/ls_src1	LS	cluster1://cluster1-vs1/ls_mr1	Snapmirrored									
			Idle	-							true	-
		cluster1://cluster1-vs1/ls_mr2	Snapmirrored									
			Idle	-							true	-

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](#)

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

Trademark information

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