



Prepare for an ONTAP upgrade

ONTAP 9

NetApp
November 01, 2023

This PDF was generated from <https://docs.netapp.com/us-en/ontap/upgrade/prepare.html> on November 01, 2023. Always check docs.netapp.com for the latest.

Table of Contents

- Prepare for an ONTAP upgrade 1
 - Prepare for an ONTAP upgrade 1
 - Create an ONTAP upgrade plan 1
 - Choose your target ONTAP release for an upgrade 2
 - Confirm ONTAP support for your hardware configuration 3
 - Identify configuration errors with Active IQ Config Advisor 3
 - Supported ONTAP upgrade paths 4
 - Verify the LIF failover configuration 27
 - Verify SVM routing configuration 29
 - Special considerations 29
 - Reboot SP or BMC to prepare for firmware update during an ONTAP upgrade 49

Prepare for an ONTAP upgrade

Prepare for an ONTAP upgrade

Properly preparing for an ONTAP 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, 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, your need for certain features, or your need to be at the minimum release to meet your 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.

- Feature availability

If you want to upgrade to the minimum ONTAP release required to support a specific feature, see the [ONTAP release recommendations](#) to determine the ONTAP version you should upgrade to.

- 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 configuration can support the target 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 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. See [NetApp Hardware Universe](#) to verify that your platform is supported for the target upgrade release.

Use these guidelines to upgrade on-premises ONTAP and ONTAP Select. For information about upgrading ONTAP in the cloud, see [Upgrading Cloud Volumes ONTAP software](#).

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**. Unless otherwise noted, these paths apply to all [upgrade methods](#); nondisruptive or disruptive, automated or manual.

• 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

These upgrade paths apply to on-premises ONTAP and ONTAP Select.



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.

Detailed upgrade paths are available for the following scenarios:

- Automated nondisruptive upgrades (ANDU) within the ONTAP 9 release family (recommended).
- Manual nondisruptive and disruptive upgrades within the ONTAP 9 release family.
- Upgrades from Data ONTAP 8.* releases to ONTAP 9 releases.

Upgrade images for some earlier releases are no longer available.

ANDU paths, ONTAP 9

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.12.1	9.13.1	direct
9.11.1	9.13.1	direct
	9.12.1	direct
9.10.1	9.13.1	direct
	9.12.1	direct
	9.11.1	direct
9.9.1	9.13.1	direct
	9.12.1	direct
	9.11.1	direct
	9.10.1	direct
9.8 Attention MetroCluster IP configurations upgrading from ONTAP 9.8: 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. <ul style="list-style-type: none"> • 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.	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

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.7	9.13.1	multi-stage -9.7 → 9.8 -9.8 → 9.12.1 -9.12.1 → 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
9.6	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

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.5	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

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

		9.5 → 9.6 - 9.5 → 9.6
	9.5	multi-stage
If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is... - 9.5 → 9.6
	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		

		9.5 and 9.6)
	9.5	multi-stage
If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
		- 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		

	9.7	multi-stage - 9.0 → 9.1 - 9.1 → 9.3
If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
	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 paths, ONTAP 9

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.12.1	9.13.1	direct
9.11.1	9.13.1	direct
	9.12.1	direct
9.10.1	9.13.1	direct
	9.12.1	direct
	9.11.1	direct
9.9.1	9.13.1	direct
	9.12.1	direct
	9.11.1	direct
	9.10.1	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.8	9.13.1	multi-stage - 9.8 → 9.12.1 - 9.12.1 → 9.13.1
Attention MetroCluster IP configurations upgrading from ONTAP 9.8: 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. <ul style="list-style-type: none"> • FAS2750 • FAS500f • AFF A220 • AFF A250 Clusters in MetroCluster IP configurations on these platforms cannot be upgraded directly from 9.8 to 9.10.1 or later. The listed direct upgrade paths can be used for all other platforms.	9.12.1	direct
	9.11.1	direct
	9.10.1	direct
	9.9.1	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.7	9.13.1	multi-stage -9.7 → 9.8 -9.8 → 9.12.1 -9.12.1 → 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
9.6	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

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.5	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

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.4	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 manual upgrade path is...
9.3	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 manual upgrade path is...
9.2		

	9.6	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
	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 manual upgrade path is...
9.1		

	9.6	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
	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 manual upgrade path is...
9.0		

	9.7	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7
If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
	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

Upgrade paths, 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.

Batch and rolling upgrades

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.

Verify your LIF failover configuration

- 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
      Logical      Home      Failover      Failover
Vserver  Interface  Node:Port      Policy      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-vsimsim-ucs572q:e0d,sti8-vsimsim-ucs572r:e0d
```

Related information

[Network and LIF management](#)

Verify SVM routing configuration

It is a best practice to configure one default route for an SVM. To avoid disruption, before you upgrade ONTAP, you should ensure that the default route is able to reach any network address that is not reachable by a more specific route. 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.

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?	<ul style="list-style-type: none"> • Prepare your SnapMirror relationships for upgrade • 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
Do I have deduplicated volumes and aggregates?	Verify you have enough free space for your deduplicated volumes and aggregates
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
Is SSL FIPS mode enabled on a cluster where administrator accounts authenticate with an SSH public key?	Verify SSH host key algorithm support
Am I upgrading from ONTAP 9.3?	Prepare all load-sharing mirrors

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. 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 destruction 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 FAS8000 running ONTAP 9.5 and you are adding a new C-Series platform running ONTAP 9.12.1, you should upgrade your FAS8000 to ONTAP 9.8 (which is the maximum ONTAP version it supports).

2. Add the new nodes to your cluster.

Use the ONTAP command `cluster add-node -allow-mixed-version-join` at the advanced privilege level to join the new nodes.

3. [Migrate the data](#) from any nodes that cannot be upgraded to a node running the higher ONTAP version.
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](#)

Upgrade requirements for MetroCluster configurations

When you upgrade a MetroCluster configuration, you should be aware of some important requirements.

Required methods for performing major and patch upgrades of MetroCluster configurations

Regardless of the version of ONTAP you're running, patch upgrades to MetroCluster configurations can be performed with automatic non-disruptive upgrade (ANDU) procedure.

As long as you're running ONTAP 9.3 or later, major upgrades to MetroCluster configurations can be performed with automatic non-disruptive upgrade (ANDU) procedure. On clusters running ONTAP 9.2 or earlier, major upgrades to MetroCluster configurations must be performed with the NDU procedure that is specific to MetroCluster configurations.

General 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 upgrade, the MetroCluster configuration must be in normal mode.
- If you're performing a patch 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 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 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	<code>iscsi initiator show -fields igroup,initiator-name,tpgroup</code>
FC	<code>fcp initiator show -fields igroup,wwpn,lif</code>

SnapMirror

Prepare SnapMirror relationships for an ONTAP upgrade

Before you upgrade ONTAP on a cluster that is running SnapMirror, SnapMirror operations must be quiesced for each node that contains destination volumes, and each peered SVM must have a unique name across the clusters. It is best practice to use a unique fully qualified domain name (FQDN) for each SVM, for example, “dataVerser.HQ” or “mirrorVserver.Offsite”.

You should also be aware that if you are upgrading clusters with DP SnapMirror relationships, you must upgrade the destination nodes before you upgrade the source nodes.

Quiesce SnapMirror operations before upgrading ONTAP

To prevent SnapMirror transfers from failing, you must quiesce SnapMirror operations. Alternatively, you can quiesce SnapMirror transfers on a particular destination volume and upgrade the owning destination node before upgrading source nodes so the SnapMirror transfers for all other destination volumes can continue. The following table describes the two options for suspending SnapMirror operations.

Option	Description	Upgrade destination nodes before source nodes?
Suspend SnapMirror operations for the duration of the NDU (nondisruptive upgrade).	The simplest method for upgrading in a SnapMirror environment is to suspend all SnapMirror operations, perform the upgrade, and then resume the SnapMirror operations. However, no SnapMirror transfers will occur during the entire NDU. You must use this method if your cluster contains nodes that are mirroring volumes to each other.	No, the nodes can be upgraded in any order.

Option	Description	Upgrade destination nodes before source nodes?
Suspend SnapMirror operations one destination volume at a time.	You can suspend SnapMirror transfers for a particular destination volume, upgrade the node (or HA pair) that contains the destination volume, upgrade the node (or HA pair) that contains the source volume, and then resume the SnapMirror transfers for the destination volume. By using this method, SnapMirror transfers for all other destination volumes can continue while the nodes that contain the original destination and source volumes are upgraded.	Yes.

Steps

1. Determine the destination path for each SnapMirror relationship:

```
snapmirror show
```

2. For each destination volume, suspend future SnapMirror transfers:

```
snapmirror quiesce -destination-path destination
```

If there are no active transfers for the SnapMirror relationship, this command sets its status to "Quiesced". If the relationship has active transfers, the status is set to "Quiescing" until the transfer is completed, and then the status becomes "Quiesced".

This example quiesces transfers involving the destination volume "vol1" from "SVMvs0.example.com":

```
cluster1::> snapmirror quiesce -destination-path vs0.example.com:vol1
```

3. Verify that all SnapMirror relationships are quiesced:

```
snapmirror show -status !Quiesced
```

This command displays any SnapMirror relationships that are *not* quiesced.

This example shows that all SnapMirror relationships are quiesced:

```
cluster1::> snapmirror show -status !Quiesced
There are no entries matching your query.
```

4. If any SnapMirror relationships are currently being transferred, do one of the following options:

Option	Description
Wait for the transfers to finish before performing the ONTAP upgrade.	After each transfer finishes, the relationship changes to "Quiesced" status.
Stop the transfers: <pre>snapmirror abort -destination-path destination -h</pre> Note: You must use the <code>-foreground true</code> parameter if you are terminating load-sharing mirror transfers.	This command stops the SnapMirror transfer and restores the destination volume to the last Snapshot copy that was successfully transferred. The relationship is set to "Quiesced" status.

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.



Version-independence is not supported for SVM replication.

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 (CVO) 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 CVO systems.



Interoperability is bidirectional.

Interoperability for ONTAP version 9.3 and later

ONTAP version ...	Interoperates with these previous ONTAP versions...																
	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

9.14.0*	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	No	No	No	No	No
9.13.0*	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	No	No	No	No
9.12.0*	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	No	No	No
9.11.0*	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	No	No
9.10.0*	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	No	No
9.9.0*	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.8	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
9.7	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
9.6	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	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	Yes	Yes	Yes
9.3	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...								
	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.13.1	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
9.12.1	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
9.11.1	Yes	Yes	Yes	Yes	Yes	No	No	No	No
9.10.1	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No

9.9.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.8	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No
9.7	No	No	No	No	Yes	Yes	Yes	Yes	Yes
9.6	No	No	No	No	No	Yes	Yes	Yes	Yes
9.5	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 only supported between clusters running the same version of ONTAP.

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; for example, from ONTAP 9.11.1 to ONTAP 9.12.1.
- The ONTAP version on the target cluster must be no more than 2 on premises versions newer or two 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.

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*
9.3	Yes	Yes	Yes														
9.4		Yes	Yes	Yes													
9.5			Yes	Yes	Yes												
9.6				Yes	Yes	Yes											
9.7					Yes	Yes	Yes										
9.8						Yes	Yes	Yes									
9.9.0*							Yes	Yes	Yes								
9.9.1								Yes	Yes	Yes							
9.10.0*									Yes	Yes	Yes						
9.10.1										Yes	Yes	Yes					

9.11.0*										Yes	Yes	Yes				
9.11.1											Yes	Yes	Yes			
9.12.0*												Yes	Yes	Yes		
9.12.1													Yes	Yes	Yes	
9.13.0*														Yes	Yes	Yes
9.13.1															Yes	Yes
9.14.0*																Yes

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:

You must replace the variables in angle brackets with the required values before running this command.

```
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:

You must replace the variables in angle brackets with the required values before running this command.

```
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 svml -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
svml 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:

You must replace the variables in angle brackets with the required values before running this command.

```
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:

You must replace the variables in angle brackets with the required values before running this command.

```
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:

You must replace the variables in angle brackets with the required values before running this command.

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

You must replace the variables in angle brackets with the required values before running this command.

```
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 DR 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
```

8. Resync the source and destination volumes:

You must replace the variables in angle brackets with the required values before running this command.

```
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
```

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

You must replace the variables in angle brackets with the required values before running this command.

```
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

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.

Related information

[Reconfiguring KMIP server connections after upgrading to ONTAP 9.3 or later](#)

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

Before you upgrade or revert 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 or revert 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
```

Considerations for session-oriented protocols

Clusters and session-oriented protocols might cause adverse effects on clients and applications in certain areas 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 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 enabling upgrading, or administrator authentication will fail.

[Learn more about enabling SSH public key accounts](#).

Prepare all load-sharing mirrors before upgrading from ONTAP 8.3

Before you upgrade from ONTAP 8.3, you should move all of the load-sharing mirror source volumes to an aggregate on the node that you will upgrade last. This ensures that load-sharing mirror destination volumes are the same or later versions of ONTAP.



You only need to perform this procedure when upgrading from ONTAP 8.3.

Steps

1. Record the locations of all load-sharing mirror source volumes.

Knowing where the load-sharing mirror source volumes came from helps facilitate returning them to their original locations after the major upgrade.

2. Determine the node and aggregate to which you will move the load-sharing mirror source volumes.
3. Move the load-sharing mirror source volumes to the node and aggregate by using the volume move start command.

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](#)

Copyright information

Copyright © 2023 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.