



Upgrade cluster

ONTAP 9

NetApp
May 18, 2021

This PDF was generated from https://docs.netapp.com/us-en/ontap/upgrade/concept_upgrade_paths.html on May 18, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Upgrade ONTAP 1
 - What version of ONTAP can I upgrade to? 1
 - How to plan your upgrade 2
 - What to check before upgrading 7
 - Download and install the ONTAP software image 30
 - Which upgrade method should I use? 33
 - What to do after upgrading 74

Upgrade ONTAP

The [method you use to upgrade](#) your ONTAP software depends upon your configuration. If it is supported by your configuration, you should perform an automated nondisruptive upgrade (ANDU) using System Manager.

If you have an active [SupportEdge](#) contract for [Active IQ Digital Advisor](#), before you begin your upgrade, you should launch Upgrade Advisor in Active IQ Digital Advisor to help you plan your upgrade.

The content in this section will guide you through the steps you should take before and after you upgrade, including the resources you should read and the necessary pre- and post-upgrade checks you should perform.

What version of ONTAP can I upgrade to?

The version of ONTAP that you can upgrade to varies based on the version of ONTAP currently running on your nodes. You can determine the current version of ONTAP running on each node by using the `system image show` command.

You can upgrade from...	To...
ONTAP 9.9.0	ONTAP 9.9.1
ONTAP 9.8	ONTAP 9.9.0 or 9.9.1
ONTAP 9.7	ONTAP 9.8 or 9.9.1
ONTAP 9.6	ONTAP 9.7 or 9.8
ONTAP 9.5	ONTAP 9.6, 9.7, or 9.9.1 Note: If you are upgrading from ONTAP 9.5 directly to 9.9.1, you must download the software image for ONTAP 9.7 and 9.9.1. The automated upgrade process uses the 9.7 image in the background to complete the update to 9.9.1. You should expect multiple reboots during the process.
ONTAP 9.4	ONTAP 9.5
ONTAP 9.3	ONTAP 9.4, 9.5 or 9.7 Note: If you are upgrading from ONTAP 9.3 directly to 9.7, you must download the software image for ONTAP 9.5 and 9.7. The automated upgrade process uses the 9.5 image in the background to complete the update to 9.7. You should expect multiple reboots during the process.
ONTAP 9.2	ONTAP 9.3

You can upgrade from...	To...
ONTAP 9.1	ONTAP 9.2 or 9.3
ONTAP 9	ONTAP 9.1
Data ONTAP 8.3.x	ONTAP 9 or 9.1
Data ONTAP 8.2.x or earlier	Data ONTAP 8.3.x
Note: If you are running a release earlier than Data ONTAP 8.3.x, you cannot upgrade directly to ONTAP 9 or 9.1. You must upgrade to Data ONTAP 8.3.x first, then upgrade to ONTAP 9 or 9.1.	

How to plan your upgrade

You should use Upgrade Advisor, one of the services provided in NetApp [Active IQ](#) to plan your upgrade. Without Upgrade Advisor, you need to perform additional manual checks before upgrading.

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.



An active SupportEdge contract is required for Active IQ.

1. [Launch Active IQ](#)
2. Review the Active IQ health summary to help assess the health of your cluster.
3. Review the recommended upgrade path and generate your upgrade plan.

Related information

[SupportEdge Services](#)

Plan your upgrade without Upgrade Advisor

It is a best practice to use Upgrade Advisor in [Active IQ](#) to plan your upgrade. If you do not have an active [SupportEdge](#) contract for Active IQ, you should perform the necessary pre-upgrade checks and create your own upgrade plan.

How long will my 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.

Our 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. However, the actual duration of your upgrade process will depend on your individual environment and the number of nodes.

Resources to read before you upgrade

If you don't use [Active IQ Upgrade Advisor](#), you need to review a number of NetApp resources before upgrading your ONTAP software. These resources will help you understand issues you must resolve, new system behavior in the target release, and confirm hardware support.

1. Review the *Release Notes* for the target release.

[ONTAP 9 Release Notes](#)

The “Important cautions” section describes potential issues that you should be aware of before upgrading to the new release. The “New and changed features” and “Known problems and limitations” sections describe new system behavior after upgrading to the new release.

2. Confirm that your hardware platform is supported in the target release.

[NetApp Hardware Universe](#)

3. Confirm that your cluster and management switches are supported in the target release.

Your NX-OS (cluster network switches), IOS (management network switches), and reference configuration file (RCF) software versions must be compatible with the version of ONTAP to which you are upgrading.

[NetApp Interoperability Matrix Tool](#)

4. If your cluster and management switches do not have the minimum software versions for the target ONTAP release, upgrade to supported software versions.

[NetApp Downloads: Cisco Ethernet Switch](#)

[NetApp Downloads: NetApp Ethernet Switch](#)

5. If your cluster is configured for SAN, 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.

[NetApp Interoperability Matrix Tool](#)

6. If you are transitioning from 7-Mode using the 7-Mode Transition Tool, confirm that the tool supports transition to the ONTAP version to which you are upgrading.

All the projects in the tool must be in the completed or aborted state before you upgrade the 7-Mode Transition Tool that supports the ONTAP version to which you are upgrading.

[7-Mode Transition Tool installation and administration](#)

What to verify before upgrading

If you don't use [Active IQ](#) Upgrade Advisor to plan your upgrade, you should verify your cluster upgrade limits and your cluster activity before you upgrade.

Verify cluster upgrade limits

If you don't use [Active IQ](#) Upgrade Advisor, you need to verify that your cluster does not exceed the platform system limits. SAN also has limits that you should verify in addition to the platform system limits.

1. Verify that the cluster does not exceed the system limits for your platform.

[NetApp Hardware Universe](#)

2. If your cluster is configured for SAN, verify that it does not exceed the configuration limits for FC, FCoE, and iSCSI.

[NetApp Hardware Universe](#)

3. Determine the CPU and disk utilization: `node run -node node_name -command sysstat -c 10 -x 3`

You should monitor CPU and disk utilization for 30 seconds. The values in the **CPU** and **Disk Util** columns should not exceed 50% for all 10 measurements reported. No additional load should be added to the cluster until the upgrade is complete. NOTE: CPU and disk utilization can vary at different times in your environment. Therefore, it is best to check your CPU and disk utilization during the timeframe of your anticipated upgrade window.

Verify current cluster activity

If you don't use [Active IQ](#) Upgrade Advisor, before upgrading, you should manually verify that no jobs are running and that any CIFS sessions that are not continuously available are terminated.

Verify that no jobs are running

Before upgrading the ONTAP software, you must verify the status of cluster jobs. If any aggregate, volume, NDMP (dump or restore), or Snapshot jobs (such as create, delete, move, modify, replicate, and mount jobs) are running or queued, you must allow the jobs to finish successfully or stop the queued entries.

1. Review the list of any running or queued aggregate, volume, or Snapshot jobs: `job show`

```
cluster1::> job show
```

Job ID	Name	Owning Vserver	Node	State
8629	Vol Reaper	cluster1	-	Queued
Description: Vol Reaper Job				
8630	Certificate Expiry Check	cluster1	-	Queued
Description: Certificate Expiry Check				
.				
.				
.				

2. Delete any running or queued aggregate, volume, or Snapshot copy jobs: `job delete -id job_id`

```
cluster1::> job delete -id 8629
```

3. Verify that no aggregate, volume, or Snapshot jobs are running or queued: `job show`

In this example, all running and queued jobs have been deleted:

```
cluster1::> job show
```

Job ID	Name	Owning Vserver	Node	State
9944	SnapMirrorDaemon_7_2147484678	cluster1	node1	Dormant
Description: Snapmirror Daemon for 7_2147484678				
18377	SnapMirror Service Job	cluster1	node0	Dormant
Description: SnapMirror Service Job				
2 entries were displayed				

Identifying active CIFS sessions that should be terminated

Before upgrading the ONTAP software, you should identify and gracefully terminate any CIFS sessions that are not continuously available.

Continuously available CIFS shares, which are accessed by Hyper-V or Microsoft SQL Server clients using the SMB 3.0 protocol, do not need to be terminated before upgrading.

1. Identify any established CIFS sessions that are not continuously available: `vserver cifs session show -continuously-available Yes -instance`

This command displays detailed information about any CIFS sessions that have no continuous availability.

You should terminate them before proceeding with the ONTAP upgrade.

```
cluster1::> vserver cifs session show -continuously-available Yes
-instance

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
Workstation IP address: 203.0.113.20
Authentication Mechanism: NTLMv2
Windows User: CIFSLAB\user1
UNIX User: nobody
Open Shares: 1
Open Files: 2
Open Other: 0
Connected Time: 8m 39s
Idle Time: 7m 45s
Protocol Version: SMB2_1
Continuously Available: No
1 entry was displayed.
```

2. If necessary, identify the files that are open for each CIFS session that you identified: `vserver cifs session file show -session-id session_ID`

```
cluster1::> vserver cifs session file show -session-id 1

Node:      node1
Vserver:   vs1
Connection: 4160072788
Session:   1
File      File      Open Hosting
Continuously
ID        Type      Mode Volume      Share      Available
-----
-----
1         Regular   rw   vol10          homedirshare   No
Path: \TestDocument.docx
2         Regular   rw   vol10          homedirshare   No
Path: \file1.txt
2 entries were displayed.
```

Related information

What to check before upgrading

Even if you use [Active IQ Upgrade Advisor](#) to plan your upgrade, there still are various pre-checks you should perform before you upgrade.

Verify cluster health

Before 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. Enter `y` to continue.
4. 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	<code>cluster ring show -unitname mgmt</code>
Volume location database	<code>cluster ring show -unitname vlodb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

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.

- If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -messagename scsiblade.*`

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show -messagename scsiblade.*
```

Time	Node	Severity	Event
MM/DD/YYYY TIME	node0	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...
MM/DD/YYYY TIME	node1	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...

- Return to the admin privilege level: `set -privilege admin`

Related information

[System administration](#)

Verify storage health

Before and after you upgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

- Verify disk status:

To check for...	Do this...
Broken disks	<ol style="list-style-type: none"> Display any broken disks: <code>storage disk show -state broken</code> Remove or replace any broken disks.
Disks undergoing maintenance or reconstruction	<ol style="list-style-type: none"> Display any disks in maintenance, pending, or reconstructing states: <code>storage disk show -state maintenance</code>

To check for...	Do this...
pending	reconstructing` .. Wait for the maintenance or reconstruction operation to finish before proceeding. +

2. Verify that all aggregates are online by displaying the state: `storage aggregate show -state !online`

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verify that all volumes are online by displaying any volumes that are *not* online: `volume show -state !online`

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

If any inconsistent volumes are returned, you must contact NetApp Support before you precede with the upgrade.

Related information

[Logical storage management](#)

Verify SVM routing configuration

It is a best practice to configure one default route for an SVM. To avoid disruption, 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 clustered 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 is especially an issue if you have configured multiple default routes.

Verifying the LIF failover configuration

Before you perform an upgrade, you must verify that the 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 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 "failed" node, 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.

- 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's first attempts to fail over to port e0c on node0. If lif0 cannot fail over to e0c, it next 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 status

Before you upgrade, you should verify the following:

- HA pair status
- LDAP status (for ONTAP 9.2 or later)
- DNS server status (for ONTAP 9.2 or later),
- Networking and storage status (for MetroCluster configurations)

Verifying HA status

Before performing a nondisruptive upgrade, you should verify that storage failover is enabled for each HA pair. If the cluster consists of only two nodes, you should also verify that cluster HA is enabled.

You do not need to verify the HA status if you plan to perform a disruptive upgrade, because this upgrade method does not require storage failover.

1. Verify that storage failover is enabled and possible for each HA pair: `storage failover show`

This example shows that storage failover is enabled and possible on node0 and node1:

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

Node	Partner	Takeover Possible	State
node0	node1	true	Connected to node1
node1	node0	true	Connected to node0

2 entries were displayed.

If necessary, you can enable storage failover by using the storage failover modify command.

2. If the cluster consists of only two nodes (a single HA pair), verify that cluster HA is configured: `cluster ha show`

This example shows that cluster HA is configured:

```
cluster1::> cluster ha show
High Availability Configured: true
```

If necessary, you can enable cluster HA by using the cluster ha modify command.

Verifying LDAP status (ONTAP 9.2 and later)

Beginning in ONTAP 9.2, if LDAP is used by your storage virtual machines (SVMs), you must have an established LDAP connection to perform a nondisruptive upgrade. You should verify the LDAP connection before you begin the upgrade.

The task does not apply if you are upgrading from ONTAP 9.1 or earlier.

1. Check the LDAP status: `ldap check -vserver vservice_name`

2. If the LDAP status is down, modify it: `ldap client modify -client-config LDAP_client -ldap -servers ip_address`
3. Verify that the LDAP status is up: `ldap check -vserver vservice_name`

Verifying DNS server status (ONTAP 9.2 and later)

Beginning in ONTAP 9.2 and later, you should verify the status of your Domain Name Service (DNS) server before and after performing a nondisruptive upgrade.

The task does not apply if you are upgrading from ONTAP 9.1 or earlier.

1. Check the status of your DNS servers: `dns check -vserver vservice_name`

An up status indicates the service is running. A down status indicates that the service is not running.

2. If the DNS server is down, modify it: `dns modify -vserver vservice_name -domains domain_name -name-servers name_server_ipaddress`
3. Verify the status of the DNS server is up.

Verifying networking and storage status for MetroCluster configurations

Before and after performing an update 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`

If any inconsistent volumes are returned, you must contact NetApp Support before you precede with the upgrade.

Verify all LIFS are on home ports before upgrade

During a reboot, some LIFs might have been migrated to their assigned failover ports. Before and after you upgrade a cluster, you must enable and revert any LIFs that are not on their home ports.

The network interface revert command reverts a LIF that is not currently on its home port back to its home port, provided that the home port is operational. A LIF's home port is specified when the LIF is created; you can determine the home port for a LIF by using the network interface show command.

1. Display the status of all LIFs: `network interface show`

This example displays the status of all LIFs for a storage virtual machine (SVM).

```
cluster1::> network interface show -vserver vs0
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
vs0					
	data001	down/down	192.0.2.120/24	node0	e0e
true					
	data002	down/down	192.0.2.121/24	node0	e0f
true					
	data003	down/down	192.0.2.122/24	node0	e2a
true					
	data004	down/down	192.0.2.123/24	node0	e2b
true					
	data005	down/down	192.0.2.124/24	node0	e0e
false					
	data006	down/down	192.0.2.125/24	node0	e0f
false					
	data007	down/down	192.0.2.126/24	node0	e2a
false					
	data008	down/down	192.0.2.127/24	node0	e2b
false					

8 entries were displayed.

If any LIFs appear with a Status Admin status of down or with an Is home status of false, continue with the next step.

2. Enable the data LIFs: `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.
```

3. Revert LIFs to their home ports: `network interface revert *`

This command reverts all LIFs back to their home ports.

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

4. Verify that all LIFs are in their home ports: `network interface show`

This example shows that all LIFs for SVM vs0 are on their home ports.

```
cluster1::> network interface show -vserver vs0
```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
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.

Use Config Advisor to verify there are no common configuration errors

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

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



Support for Config Advisor is limited and is available only online.

1. Log in to the NetApp Support Site, and then navigate to **Downloads > Software > ToolChest**.
2. Click [Config Advisor](#).
3. Download, install, and run Config Advisor by following the directions on the web page.
4. After running Config Advisor, review the tool's output, and follow the recommendations that are provided to address any issues that are discovered by the tool.

Pre-upgrade checks

Depending on your environment, you need to consider certain factors before you start

your upgrade. Get started by reviewing the table below to see what special considerations you need to consider.

Ask yourself...	If your answer is yes, then do this...
Do I have a mixed version cluster?	Check mixed version requirements
Do I have a SAN configuration?	Verify the SAN configuration
Do I have a MetroCluster configuration?	<ul style="list-style-type: none">• Review specific upgrade requirements for MetroCluster configurations• Verify networking and storage status
Are nodes on my cluster using root-data partitioning and root-data-data-partitioning?	Examine upgrade considerations for root-data and root-data-data partitioning
Do I have deduplicated volumes and aggregates?	Verify you have enough free space for your deduplicated volumes and aggregates
Is my cluster running SnapMirror?	<ul style="list-style-type: none">• Review upgrade requirements for SnapMirror• Prepare your SnapMirror relationships for upgrade
Is my cluster running SnapLock?	Review upgrade considerations for SnapLock
Am I upgrading from ONTAP 8.3 and have load-sharing mirrors	Prepare all load-sharing mirrors for upgrade
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

Mixed version requirements

Beginning with ONTAP 9.3, by default, you cannot join new nodes to the cluster that are running a version of ONTAP that is different from the version running on the existing nodes.

If you plan to add new nodes to your cluster that are running a version of ONTAP that is later than the nodes in your existing cluster, you should upgrade the nodes in your cluster to the later version first, then add the new nodes.

Mixed version clusters are not recommended, but in certain cases you might need to temporarily enter a mixed version state. For example, you need to enter a mixed version state if you are upgrading to a later version of ONTAP that is not supported on certain nodes in your existing cluster. In this case, you should upgrade the nodes that do support the later version of ONTAP, then unjoin the nodes that do not support the version of ONTAP you are upgrading to using the advance privilege `cluster unjoin -skip-lastlow-version -node check` command.

You might also need to enter a mixed version state for a technical refresh or an interrupted upgrade. In such cases you can override the ONTAP 9.3 default behavior and join nodes of a different version using the following advance privilege commands:

- `cluster join -allow-mixed-version-join`
- `cluster add-node -allow-mixed-version-join`

When you have to enter a mixed version state, you should complete the upgrade as quickly as possible. An HA pair must not run an ONTAP version from a release that is different from other HA pairs in the cluster for more than seven days. For correct cluster operation, the period the cluster is in a mixed version state should be as short as possible.

When the cluster is in a mixed version state, you should not enter any commands that alter the cluster operation or configuration except as necessary to satisfy the upgrade requirements.

Verifying the SAN configuration

Upgrading in a SAN environment changes which paths are direct. Therefore, before performing an upgrade, 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.

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>fc initiator show -fields igroup, wwn, lif</code>

MetroCluster configurations

Upgrade requirements for MetroCluster configurations

If you have to upgrade a MetroCluster configuration, you should be aware of some important requirements.

Required methods for performing major and minor upgrades of MetroCluster configurations

Patch upgrades to MetroCluster configurations can be performed with automatic non-disruptive upgrade (NDU) procedure.

Starting with ONTAP 9.3, major upgrades to MetroCluster configurations can be performed with automatic non-disruptive upgrade (NDU) procedure. On systems 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.

- The MetroCluster configuration must be in either normal or switchover mode.



Upgrade in switchover mode is only supported in minor patch upgrades.

- 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 networking and storage status for MetroCluster configurations

Before performing an upgrade 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
```

	Logical	Status	Network	Current	
Current Is					
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`

If any inconsistent volumes are returned, you must contact NetApp Support before you precede with the upgrade.

Related information

[Upgrade requirements for MetroCluster configurations](#)

Upgrade considerations for root-data partitioning and root-data-data partitioning

Root-data partitioning and root-data-data-partitioning is supported for some platform models and configurations. This partitioning capability is enabled during system initialization; it cannot be applied to existing aggregates.

For information about migrating your data to a node that is configured for root-data partitioning or root-data-data partitioning, contact your account team or partner organization.

Related information

[ONTAP concepts](#)

Verify that deduplicated volumes and aggregates contain sufficient free space

Before upgrading ONTAP, you must verify that any deduplicated volumes and the aggregates that contain them have sufficient free space for the deduplication metadata. If there is insufficient free space, deduplication will be disabled when the ONTAP upgrade is completed.

Each deduplicated volume must contain at least 4% free space. Each aggregate that contains a deduplicated

volume must contain at least 3% free space.

1. Determine which volumes are deduplicated: `volume efficiency show`
2. Determine the free space available on each volume that you identified: `vol show -vserver Vserver_name -volume volume_name -fields volume, size, used, available, percent-used, junction-path`

Each deduplicated volume must not contain more than 96% used capacity. If necessary, you can increase the sizes of any volumes that exceed this capacity.

Logical storage management

In this example, the percent-used field displays the percentage of used space on the deduplicated volume.:

```
vserver      volume size      junction-path available used      percent-used
-----
cluster1-01 vol0      22.99GB -              14.11GB      7.73GB 35%
cluster1-02 vol0      22.99GB -              12.97GB      8.87GB 40%
2 entries were displayed.
```

3. Identify the free space available on each aggregate that contains a deduplicated volume: `aggr show -aggregate aggregate_name -fields aggregate, size, usedsize, availsize, percent-used`

Each aggregate must not contain more than 97% used capacity. If necessary, you can increase the sizes of any aggregates that exceed this capacity.

Disk and aggregate management

In this example, the percent-used field displays the percentage of used space on the aggregate containing the deduplicated volume (aggr_2):

```
aggr show -aggregate aggregate_name -fields
aggregate, size, usedsize, availsize, percent-used
aggregate          availsize percent-used size      usedsize
-----
aggr0_cluster1_01  1.11GB   95%          24.30GB 23.19GB
aggr0_cluster1_02 1022MB   96%          24.30GB 23.30GB
2 entries were displayed.
```

SnapMirror

Upgrade requirements for SnapMirror

You must perform certain tasks to successfully upgrade a cluster that is running SnapMirror.

- If you are upgrading clusters with an inter-cluster DP SnapMirror relationship, you must upgrade the destination cluster before you upgrade the source cluster.
- Before upgrading 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.

For SnapMirror volume replication, the destination node must use an ONTAP version that is equal to or later than that of the SnapMirror source node. To prevent SnapMirror transfers from failing, you must suspend SnapMirror operations and, in some cases, upgrade destination nodes before upgrading source nodes. 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.
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.

SVM peering requires SVM names to be unique across clusters. It is best practice to name SVMs with a unique fully qualified domain name (FQDN), for example, “dataVerser.HQ” or “mirrorVserver.Offsite”. Using the FQDN naming style makes it much easier to make sure of uniqueness.

Related information

[ONTAP concepts](#)

Prepare SnapMirror relationships for a nondisruptive upgrade

It is recommended that you quiesce your SnapMirror operations before performing a nondisruptive upgrade of ONTAP.

- 1. Use the `snapmirror show` command to determine the destination path for each SnapMirror relationship.
- 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: <code>snapmirror abort -destination-path destination -h</code> Note: You must use the <code>-foreground true</code> parameter if you are aborting 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.

Related information

[Upgrade requirements for SnapMirror](#)

Upgrade considerations for SnapLock

SnapLock does not allow the download of certain kernel versions if these are qualified as bad SnapLock releases or if SnapLock is disabled in those releases. These download restrictions only apply if the node has SnapLock data.

Prepare all load-sharing mirrors for a major upgrade

Before performing a major 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.

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.

Delete existing external key management server connections before upgrading

If you are using NetApp Storage Encryption (NSE) on ONTAP 9.2 or earlier 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 before performing the upgrade.

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.

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](#)

Verifying that the netgroup file is present on all nodes

If you have loaded netgroups into storage virtual machines (SVMs), before you upgrade or revert, 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.

The *NFS Reference* contains more information about netgroups and loading them from a URI.

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

[NFS management](#)

Configure LDAP clients to use TLS for highest security

Before upgrading to the target ONTAP release, 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.

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`

Download and install the ONTAP software image

You must first download the ONTAP software from the NetApp Support site; then you can install it.

Download the software image

For ONTAP 9.4 and later, you can copy the ONTAP software image from the NetApp Support Site to a local folder. For upgrades from ONTAP 9.3 or earlier, you must copy the ONTAP software image to an HTTP server or FTP server on your network.

You should note the following important information:

- Software images are specific to platform models.

You must obtain the correct image for your cluster. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site.

- Software images include the latest version of system firmware that was available when a given version of ONTAP was released.
- If you are 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.

- If you are upgrading from ONTAP 9.5 to 9.9.1, you must copy the software image for ONTAP 9.7 and 9.9.1.
- If you are upgrading from ONTAP 9.3 to 9.7, you must copy the software image for ONTAP 9.5 and 9.7.
 1. Locate the target ONTAP software in the [Software Downloads](#) area of the NetApp Support Site.
 2. Copy the software image.
 - For ONTAP 9.3 or earlier, copy the software image (for example, 93_q_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served.
 - For ONTAP 9.4 or later, copy the software image (for example, 97_q_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served or to a local folder.

Install the software image

You must install the target software image on the cluster's nodes.

- If you are upgrading a system with NetApp Volume Encryption to ONTAP 9.5 or later, you must have downloaded the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

If you use the ONTAP software image for restricted countries to upgrade a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

- If you are upgrading from ONTAP 9.5 directly to 9.9.1, you must download the software image for ONTAP 9.7 and 9.9.1. If you are upgrading from ONTAP 9.3 directly to 9.7, you must download the software image for ONTAP 9.5 and 9.7.

The automated upgrade process uses both images in the background to complete the upgrade.

1. Set the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (***>**) appears.

For automatic nondisruptive upgrade (ANDU)

1. Check the image repository and delete any previous images.

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

```
cluster image package show-repository\  
<<smoke6-vsimg-ucs6b4c#c-login_27|There are no packages in the  
repository.\r\n
```

2. Download the image.

```
cluster image package get -url url_to_image_on_nss
```

Example

```
cluster image package get -url http://10.60.132.98/x/eng/rlse/DOT/9.7P13X2/  
promo/9.7P13X2/x86_64.optimize/image.tgz
```

3. Verify the package is downloaded.

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

Example

```
cluster image package show-repository -fields download-ver\  
<<smoke6-vsimg-ucs6b4c#c-login_27| download-verX;X\r\n  
<<smoke6-vsimg-ucs6b4c#c-login_27| Downloaded VersionX;X\r\n  
<<smoke6-vsimg-ucs6b4c#c-login_27| Stormking__9.10.0X;X\r\n
```

For manual upgrades

1. Download the image.
 - a. If you are upgrading a non-MetroCluster configuration or a two-node MetroCluster configuration use the following command to download the image:

```
system node image update -node * -package location -replace-package true  
-setdefault true -background true
```



This command downloads and installs the software image on all of the nodes simultaneously. To download and install the image on each node one at a time, do not specify the `-background` parameter.

- b. If you are upgrading a four or eight-node MetroCluster configuration, you must issue the following command on both clusters:

```
system node image update -node * -package location -replace-package true  
true -background true -setdefault false
```

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

2. Enter `y` to continue when prompted.
3. Verify that the software image is downloaded and installed on each node.

```
system node image show-update-progress -node *
```

This command displays the current status of the software image download and installation. You should continue to run this command until all nodes report a **Run Status** of **Exited**, and an **Exit Status** of **Success**.

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

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

```
cluster1::*> system node image show-update-progress -node *  
There is no update/install in progress  
Status of most recent operation:  
    Run Status:      Exited  
    Exit Status:     Success  
    Phase:           Run Script  
    Exit Message:    After a clean shutdown, image2 will be set as  
the default boot image on node0.  
There is no update/install in progress  
Status of most recent operation:  
    Run Status:      Exited  
    Exit Status:     Success  
    Phase:           Run Script  
    Exit Message:    After a clean shutdown, image2 will be set as  
the default boot image on node1.  
2 entries were acted on.
```

Which upgrade method should I use?

The method you use to upgrade depends upon your configuration. If available, the automated nondisruptive upgrade (ANDU) using System Manager is the preferred method.

- **Nondisruptive upgrade:** In a nondisruptive upgrade, update procedures are performed in the background while maintaining service to clients. Nondisruptive upgrades can be performed using an automated or manual method.
 - **Automated nondisruptive upgrade (ANDU)** can be executed using System Manager or the ONTAP command line interface (CLI). If available for your configuration, ANDU using System Manager is the recommended method of upgrade. With ANDU, 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 the upgrade in the background.
 - **Manual nondisruptive upgrade** involves manual steps to confirm the ONTAP configuration on each node and then uses the rolling update method to perform the upgrade. In the rolling update method, 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, this time on the partner node. Each additional HA pair is upgraded in sequence until all HA pairs are running the target release. Manual nondisruptive upgrades are executed using the ONTAP CLI.
- **Disruptive:** In a disruptive upgrade, storage failover is disabled for each HA pair, and then each node is rebooted one at a time. Disruptive upgrades can be performed more quickly than nondisruptive upgrades, and require fewer steps to complete. 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.

You should only use a manual method if ANDU is not supported for your configuration.

Non-MCC configurations

The upgrade methods available for each configuration are listed in order of recommended usage.

ONTAP version	Number of nodes	Upgrade method
9.0 or later	2, 4, 8	<ul style="list-style-type: none">• Automated nondisruptive using System Manager• Automated nondisruptive using the CLI• Manual nondisruptive using the CLI (the Rolling Method)• Manual disruptive using the CLI
9.0 or later	12	<ul style="list-style-type: none">• Automated nondisruptive using the CLI• Manual nondisruptive using the CLI (the Rolling Method)• Manual disruptive using the CLI

ONTAP version	Number of nodes	Upgrade method
9.2 or later	Single-node	Automated disruptive using the CLI

MCC configurations

The upgrade methods available for each configuration are listed in order of recommended usage.

ONTAP version	Number of nodes	Upgrade method
9.3 or later	2,4	<ul style="list-style-type: none"> • Automated nondisruptive using System Manager • Automated nondisruptive using the CLI • Manual disruptive using the CLI
9.3 or later	8	<ul style="list-style-type: none"> • Automated nondisruptive using the CLI • Manual nondisruptive using the CLI • Manual disruptive using the CLI
9.2 or earlier	2	<ul style="list-style-type: none"> • Manual nondisruptive (for 2-node clusters) using the CLI • Manual disruptive using the CLI
9.2 or earlier	4, 8	<ul style="list-style-type: none"> • Manual nondisruptive using the CLI • Manual disruptive using the CLI
9.0 or later	4, 8 (patch only)	Automated nondisruptive using System Manager
9.2 or earlier	2, 4, 8 (patch only)	Automated nondisruptive using System Manager

Automated nondisruptive using System Manager

You can nondisruptively update the version of ONTAP on your cluster using System Manager.

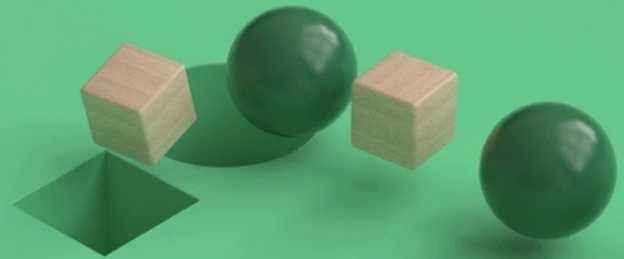
Take a look at the simplified ONTAP upgrade capabilities available in ONTAP 9.8 System Manager.

ONTAP Upgrades Made Easy

Get the transformative features you've paid for!

Tech Clip

© 2020 NetApp, Inc. All rights reserved.



The update process checks your hardware platform and configuration to verify that your system is supported by the ONTAP version to which you are upgrading. ONTAP automatically shifts workloads during an upgrade between clusters so you can continue serving data.

This procedure updates your system to the specified version of ONTAP. It is assumed that your hardware platform and configuration is supported for the target release.

Download the
software image



Upgrade ONTAP



If issues are encountered during your automated upgrade, you can view EMS messages and details in ONTAP System Manager: Click **Events & Jobs > Events**.

Steps


1. If you want to download the software image to an HTTP or FTP server on your network, copy the software image from the NetApp support site to the directory on the HTTP or FTP server from which the image will be served.

If you want to download the software image to a local folder, then click the software image on the NetApp support site, select **Save As**, and then choose the local folder to place the image.

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

ONTAP version	Steps
ONTAP 9.8 or later	Click Cluster > Overview .
ONTAP 9.5, or 9.6	Click Configuration > Cluster > Update .

ONTAP version	Steps
ONTAP 9.4 or earlier	Click Configuration > Cluster Update .

3. In the right corner of the Overview pane, click .
4. Click **ONTAP Update**.
5. 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 the local client Note: You should have already downloaded the image to the local client. Download and install the ONTAP software images	<ol style="list-style-type: none"> a. Under Available Software Images, click Add from Local. b. Browse to the location you saved the software image, select the image, and then click Open. The software image uploads after you click Open.
Add a new software image from the NetApp Support Site	<ol style="list-style-type: none"> a. Click Add from Server. b. In the Add a New Software Image dialog box, enter the URL of the HTTP server or FTP server on which you have saved the image that was downloaded from the NetApp Support Site. For anonymous FTP, you must specify the URL in the ftp://anonymous@ftpserver format. c. Click Add.
Select an available image	Choose one of the listed images.

6. Click **Validate** to run the pre-update validation checks to verify whether the cluster is ready for an update.

The validation operation checks the cluster components to validate that the update can be completed nondisruptively, and then displays any errors or warnings. It also displays any required remedial action that you must perform before updating the software.



You must perform all of the required remedial actions for the errors before proceeding with the update. Although you can ignore the remedial actions for the warnings, the best practice is to perform all of the remedial actions before proceeding with the update.

7. Click **Next**.
8. Click **Update**.

Validation is performed again.

- When the validation is complete, a table displays any errors and warnings, along with any required remedial actions to be taken before proceeding.

- If the validation is completed with warnings, you can choose to select the **Continue update with warnings** checkbox, and then click **Continue**.

When the validation is complete and the update is in progress, the update might be paused because of errors. You can click the error message to view the details, and then perform the remedial actions before resuming the update.

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

Resuming an upgrade (using System Manager) after an error in the automated upgrade process

If an automated upgrade pauses because of an error, you can resolve the error and resume the automated upgrade, or you can cancel the automated upgrade and complete the process manually. If you choose to continue the automated upgrade, do not perform any of the upgrade steps manually.

1. Depending on the System Manager version that you are running, perform one of the following steps:
 - ONTAP 9.4 or earlier: Click **Configuration** > **Cluster Update**.
 - ONTAP 9.5 or 9.6: Click **Configuration** > **Cluster** > **Update**.
 - ONTAP 9.7 or later: Click **Cluster** > **Overview**

Then in the right corner of the Overview pane, click the three blue vertical dots, and **ONTAP Update**.

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

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

Automated nondisruptive using the CLI

You can use the command line interface (CLI) to verify that the cluster can be upgraded nondisruptively, install the target ONTAP image on each node, and then, execute an upgrade in the background.

If you do not plan to monitor the progress of the upgrade process, it is a good practice to [request EMS notifications of errors that might require manual intervention](#).

- You must have met the upgrade preparation requirements.
- For each HA pair, each node should have one or more ports on the same broadcast domain.

When a set of nodes is upgraded during a batch upgrade, the LIFs are migrated to the HA partner nodes. If the partners do not have any ports in the same broadcast domain, then the LIF migration fails.

- If you are upgrading from ONTAP 9.3 to 9.7, you must have obtained the software image for 9.5 and 9.7.

- If you are upgrading from ONTAP 9.5 to 9.9.1, you must have obtained the software image for 9.7 and 9.9.1.

The cluster image validate command checks the cluster components to validate that the upgrade can be completed nondisruptively, and then provides the status of each check and any required action you must take before performing the software 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.

1. Delete the previous ONTAP software package: `cluster image package delete -version previous_ONTAP_Version`
2. Download the target ONTAP software package: `cluster image package get -url location`



If you are upgrading from ONTAP 9.3 to 9.7, download the software package for ONTAP 9.5, and then use the same command to download the software package for 9.7. If you are upgrading from ONTAP 9.5 to 9.9.1, download the software package for ONTAP 9.7, and then use the same command to download the software package for 9.9.1.

```
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              MM/DD/YYYY 10:32:15
```

4. Verify that the cluster is ready to be upgraded nondisruptively: `cluster image validate -version package_version_number`
 - If you are upgrading a two-node or four-node MetroCluster configuration, you must run this command on both clusters before proceeding.
 - If you are upgrading from ONTAP 9.3 to 9.7, use the 9.7 package for verification. You do not need to validate the 9.5 package separately.
 - If you are upgrading from ONTAP 9.5 to 9.9.1, use the 9.9.1 package for verification. You do not need to validate the 9.7 package separately.


```
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. 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 you are upgrading from ONTAP 9.3 to 9.7, use the 9.7 `package_version_number` in the above command.
 - If you are upgrading from ONTAP 9.5 to 9.9.1, use the 9.9.1 `package_version_number` in the above command.
 - For any MetroCluster configuration, except a 2-node MetroCluster system, the upgrade process starts simultaneously on both of the clusters (the disaster recovery cluster and the production cluster) after the user provides a confirmation. For a 2-node MetroCluster system, the update is started first on the disaster recovery site, that is, the site where the upgrade is not initiated. After the update is fully completed on the disaster recovery site, the upgrade begins on the production site.
 - If the cluster consists of 2 through 6 nodes, a rolling upgrade is performed. If the cluster consists of 8 or more nodes, a batch upgrade is performed by default. If desired, you can use the `-force-rolling` parameter to specify a rolling upgrade instead.
 - 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.

```

cluster1::> cluster image update -version 9.7

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::>

```

9. 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.

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

```

cluster1::> cluster image show-update-progress

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

Updated nodes: node0, node1.

cluster1::>

```

11. 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

Related information

[Launch Active IQ](#)

[Active IQ documentation](#)

Resuming an upgrade (using the CLI) after an error in the automated upgrade process

If an automated upgrade pauses because of an error, you can resolve the error and resume the automated upgrade, or you can cancel the automated upgrade and complete the process manually. If you choose to continue the automated upgrade, do not perform any of the upgrade steps manually.

If you want to manually complete the upgrade, use the cluster image cancel-update command to cancel the automated process and proceed manually. If you want to continue the automated upgrade, complete the following steps.

1. View the upgrade error: `cluster image show-update-progress`
2. Resolve the error.
3. Resume the update: `cluster image resume-update`

Automated disruptive using the CLI (single-node cluster only)

Beginning with ONTAP 9.2, you can perform an automated update of a single-node cluster. Because single-node clusters lack redundancy, updates are always disruptive.

- You must have satisfied upgrade preparation requirements.
 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.

Manual nondisruptive using the CLI

Manual nondisruptive (rolling method) using the CLI

The rolling upgrade method enables you to update a cluster of two or more nodes nondisruptively. This method has several steps: initiating a failover operation on each node in an HA pair, updating the “failed” node, initiating giveback, and then repeating the process for each HA pair in the cluster.

You must have satisfied upgrade preparation requirements.

1. Update the first node in an HA pair

You upgrade 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.

2. Update the second node in an HA pair

After upgrading or downgrading the first node in an HA pair, you upgrade its partner by initiating a takeover on it. The first node serves the partner's data while the partner node is upgraded.

3. Repeat these steps for each additional HA pair.

You should complete post-upgrade tasks.

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 state of version mismatch longer than necessary.

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, CIFS, 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, CIFS, 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.

NOTE: 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.

[High-availability configuration](#)

- 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, 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`

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, CIFS, 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, CIFS, 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.

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

NOTE: 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:

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

[High-availability configuration](#)

- b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
- c. Rerun the storage failover giveback command.

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

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

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

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

17. Verify that the update was completed successfully for the node:

- Go to the advanced privilege level :`set -privilege advanced`
- 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.

- 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
```

Current Is	Logical	Status	Network	Current	
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: `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`

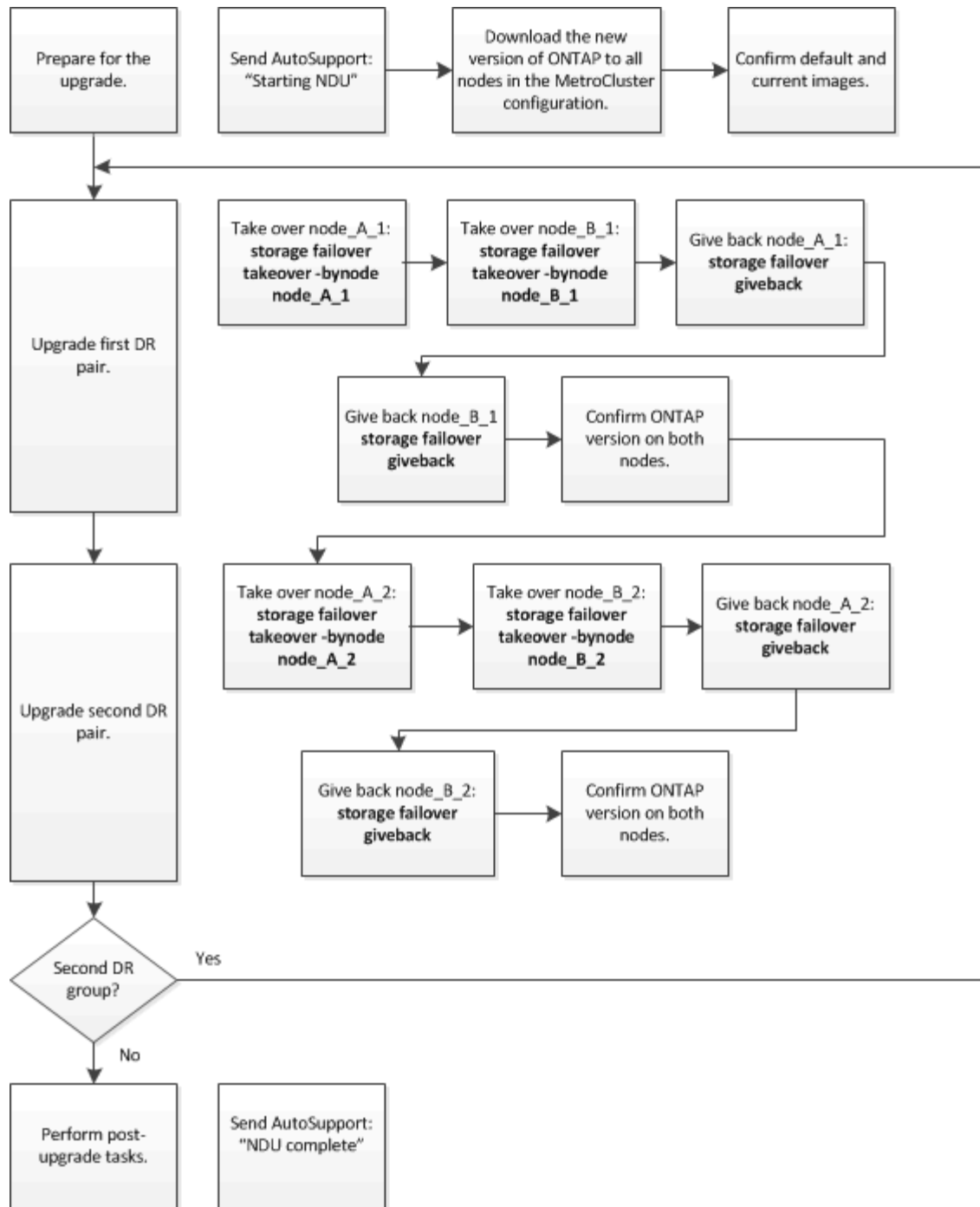
Upgrade any additional HA pairs.

MCC configurations

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

The manual update procedure for upgrading or downgrading 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 some post-update 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 software on an eight-node or four-node MetroCluster configuration

The MetroCluster software update 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:



The MetroCluster software update procedure involves upgrading or downgrading one DR group at a time.

For four-node MetroCluster configurations:

1. Update DR Group One:
 - a. Update node_A_1 and node_B_1.
 - b. Update node_A_2 and node_B_2.

For eight-node MetroCluster configurations, you perform the DR group update procedure twice:

1. Update DR Group One:
 - a. Update node_A_1 and node_B_1.
 - b. Update node_A_2 and node_B_2.
2. Update DR Group Two:
 - a. Update node_A_3 and node_B_3.
 - b. Update node_A_4 and node_B_4.

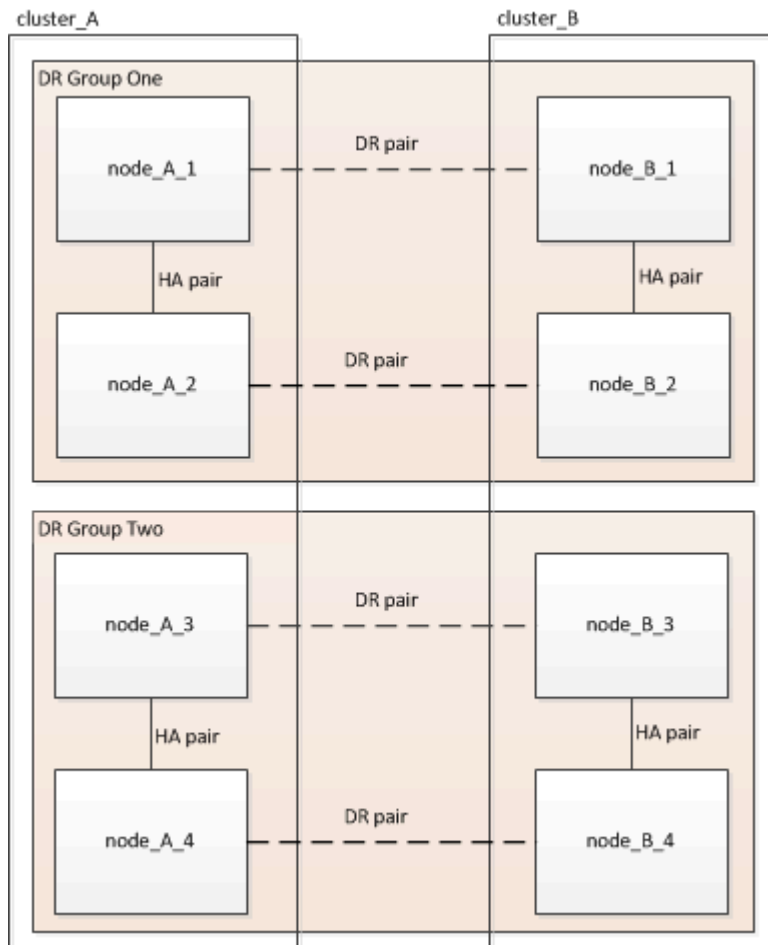
Preparing to update a MetroCluster DR group

Before you actually update the software on the nodes, you must identify the DR relationships among the nodes, send an AutoSupport message that you are initiating an update, 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 running on each node:

- a. Confirm the 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::>
```

- b. 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::>
```

4. Trigger an AutoSupport notification: `autosupport invoke -node * -type all -message "Starting_NDU"`

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

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

5. 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.

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

- a. Verify the images 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.

- b. Verify the images 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.

7. Determine whether the nodes to be upgraded are currently serving any clients by entering the following command 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.

NOTE: 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 updated.

If you have updated 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 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. Ensure 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.

- Give back the aggregates to the DR partner on cluster_A: `storage failover giveback -ofnode node_A_1`
- 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 updated.

If you have updated 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. 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:

If you are upgrading from ...	Enter this command...
ONTAP 9.1	<code>storage failover takeover -ofnode node_A_2</code>
ONTAP 9.0 or Data ONTAP 8.3.x	<code>storage failover takeover -ofnode node_A_2 -option allow-version-mismatch</code> 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.

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.

2. 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	<code>storage failover takeover -ofnode node_B_2</code>
ONTAP 9.0 or Data ONTAP 8.3.x	<code>storage failover takeover -ofnode node_B_2 -option allow-version-mismatch</code> 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.

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.

3. 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.

4. 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.

- Give back the aggregates to the DR partner on cluster_A: `storage failover giveback -ofnode node_A_2`
- 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.

5. 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.

6. 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.

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 giveback.

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

8. Set the privilege level from admin to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (***>**) appears.

9. 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::>
```

10. 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::>
```

- 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.

- 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.

Manual nondisruptive upgrade of a two-node MetroCluster configuration in ONTAP 9.2 or earlier using the CLI

You can upgrade ONTAP nondisruptively for a two-node MetroCluster configuration. This method has several steps: 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.

This procedure is for two-node MetroCluster configurations running ONTAP 9.2 or earlier only.

+

Do not use this procedure if you have a four-node MetroCluster configuration.

+

If you have a two-node MetroCluster configuration running ONTAP 9.3 or later, perform an [automated nondisruptive upgrade using System Manager](#).

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 vservers 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 showmetrocluster check config-replication showmetrocluster 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.

You should perform any post-upgrade tasks.

Related information

[MetroCluster Disaster recovery](#)

Manual disruptive 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 have satisfied preparation requirements.
- 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.

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

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, 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.

7. Verify that the upgrade is completed successfully:

- Set the privilege level to advanced: `set -privilege advanced`
- 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 upgrade is not successful, from the node, run the `system node upgrade-revert upgrade` command. If this command does not complete the node's upgrade, contact technical support immediately.

- Return to the admin privilege level: `set -privilege admin`

8. Repeat Steps 2 through 7 for each additional node.

9. 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
```

10. If the cluster consists of only two nodes, enable cluster high availability: `cluster ha modify -configured true`

What to do after upgrading

After upgrading your ONTAP software, there are several tasks you should perform to verify your cluster readiness.

Post-upgrade cluster verification

After you upgrade you should verify your cluster version, cluster health, and storage health.

Verify cluster version

After all of 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 can 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. Enter `y` to continue.
4. 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	<code>cluster ring show -unitname mgmt</code>
Volume location database	<code>cluster ring show -unitname vlddb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

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.

- If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -messagename scsiblade.*`

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show -messagename scsiblade.*
```

Time	Node	Severity	Event
MM/DD/YYYY TIME	node0	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...
MM/DD/YYYY TIME	node1	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...

- Return to the admin privilege level: `set -privilege admin`

Related information

[System administration](#)

Verify storage health

After you upgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

- Verify disk status:

To check for...	Do this...
Broken disks	<ol style="list-style-type: none"> Display any broken disks: <code>storage disk show -state broken</code> Remove or replace any broken disks.

To check for...	Do this...
Disks undergoing maintenance or reconstruction	<ol style="list-style-type: none"> Display any disks in maintenance, pending, or reconstructing states: <code>storage disk show -state maintenance pending reconstructing</code> Wait for the maintenance or reconstruction operation to finish before proceeding.

- Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates: `storage aggregate show -state !online`

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

- Verify that all volumes are online by displaying any volumes that are *not* online: `volume show -state !online`

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

- Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

If any inconsistent volumes are returned, you must contact NetApp Support before you precede with the upgrade.

Related information

[Disk and aggregate management](#)

Verify all LIFs are on home ports after upgrade

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.

The network interface revert command reverts a LIF that is not currently on its home port back to its home port, provided that the home port is operational. A LIF's home port is specified when the LIF is created; you can determine the home port for a LIF by using the network interface show command.

- Display the status of all LIFs: `network interface show`

This example displays the status of all LIFs for a storage virtual machine (SVM).

```
cluster1::> network interface show -vserver vs0
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0						
	data001	down/down	192.0.2.120/24	node0	e0e	true
	data002	down/down	192.0.2.121/24	node0	e0f	true
	data003	down/down	192.0.2.122/24	node0	e2a	true
	data004	down/down	192.0.2.123/24	node0	e2b	true
	data005	down/down	192.0.2.124/24	node0	e0e	false
	data006	down/down	192.0.2.125/24	node0	e0f	false
	data007	down/down	192.0.2.126/24	node0	e2a	false
	data008	down/down	192.0.2.127/24	node0	e2b	false

8 entries were displayed.

If any LIFs appear with a Status Admin status of "down" or with an Is home status of "false", continue with the next step.

2. Enable the data LIFs: `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up
```

8 entries were modified.

3. Revert LIFs to their home ports: `network interface revert *`

This command reverts all LIFs back to their home ports.

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

8 entries were acted on.

4. Verify that all LIFs are in their home ports: `network interface show`

This example shows that all LIFs for SVM vs0 are on their home ports.


```
cluster1::> network interface show -vserver vs0
```

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.

Post upgrade checks for special configurations

If your cluster is configured with any of the following features you might need to perform additional steps after you upgrade.

Ask yourself...	If your answer is yes, then do this...
Did I upgrade to ONTAP 9.8 or later from ONTAP 9.7 or earlier	Verify your network configuration
Do I have a MetroCluster configuration?	Verify your networking and storage status
Do I have a SAN configuration?	Verify your SAN configuration
Am I using NetApp Storage Encryption and I upgraded to ONTAP 9.3 or later?	Reconfigure KMIP server connections
Do I have load-sharing mirrors?	Relocate moved load-sharing mirror source volumes
Am I using SnapMirror?	Resume SnapMirror operations
Did I upgrade from ONTAP 8.3.0?	Set the desired NT ACL permissions display level for NFS clients
Do I have administrator accounts created prior to ONTAP 9.0?	Enforce SHA-2 on administrator passwords

Verifying your network configuration after upgrade

ONTAP 9.8 and later automatically monitors layer 2 reachability. After you upgrade from ONTAP 9.7x or earlier to ONTAP 9.8 or later, you should verify that each .network port has reachability to its expected broadcast domain.

1. Verify each port has reachability to its expected domain:

```
network port reachability show -detail
```

A reachability-status of ok indicates that the port has layer 2 reachability to its assigned domain.

Verify networking and storage status for MetroCluster configurations

After performing an update 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`

If any inconsistent volumes are returned, you must contact NetApp Support before you precede with the upgrade.

Verify the SAN configuration after an upgrade

If you are upgrading in a SAN environment, then after the upgrade, 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	<code>iscsi initiator show -fields igroup, initiator-name, tpgroup</code>
FC	<code>fcp initiator show -fields igroup, wwpn, lif</code>

Reconfiguring KMIP server connections after upgrading to ONTAP 9.3 or later

After performing an upgrade to ONTAP 9.3 or later, you must reconfigure your external key management (KMIP) server connections.

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.

Relocating moved load-sharing mirror source volumes

After successfully completing a nondisruptive upgrade, you can move load-sharing mirror source volumes back to the locations they were in originally before the upgrade.

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 by using the volume move start command.

Resuming SnapMirror operations

After completing a nondisruptive upgrade, you must resume any SnapMirror relationships that were suspended.

Existing SnapMirror relationships must have been suspended by using the `snapmirror quiesce` command, and the cluster must have been nondisruptively upgraded.

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	
Updated							
-----	----	-----	-----	-----	-----	-----	-----

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.

Setting the desired NT ACL permissions display level for NFS clients

After upgrading from ONTAP 8.3.0, the default handling for displaying NT ACL permissions to NFS clients has changed. You should check the setting and change it to the desired setting for your environment if necessary. This task does not apply if you are upgrading from ONTAP 8.3.1 or later.

In multiprotocol environments, ONTAP displays to NFS clients the permissions of NTFS security-style files and directories based on the access granted by the NT ACL to any user. In ONTAP 8.3.0, ONTAP by default displayed to NFS clients the permission based on the maximum access granted by the NT ACL. After upgrading, the default setting changes to display permissions based on the minimum access granted by the NT ACL. This change applies to new and existing storage virtual machines (SVMs).

1. Set the privilege level to advanced: `set -privilege advanced`

2. Check the setting for displaying NT ACL permissions for NFS clients: `vserver nfs show -vserver vserver_name -fields ntaccl-display-permissive-perms`

After upgrading from 8.3.0, the value for this new parameter is disabled, meaning ONTAP displays the minimum permissions.

3. If you prefer to display the maximum permissions, change the setting individually for each SVM as desired: `vserver nfs modify -vserver vserver_name -ntaccl-display-permissive-perms enabled`
4. Verify that the change took effect: `vserver nfs show -vserver vserver_name -fields ntaccl-display-permissive-perms`
5. Return to the admin privilege level: `set -privilege admin`

Enforcing SHA-2 on administrator account passwords

Administrator accounts created prior to ONTAP 9.0 continue to use MD5 passwords after the upgrade, until the passwords are manually changed. MD5 is less secure than SHA-2. Therefore, after upgrading, you should prompt users of MD5 accounts to change their passwords to use the default SHA-512 hash function.

The password hash functionality enables you to do the following:

- Display user accounts that match the specified hash function.
- Expire accounts that use a specified hash function (for example, MD5), forcing the users to change their passwords in their next login.
- Lock accounts whose passwords use the specified hash function.
- When reverting to a release earlier than ONTAP 9, reset the cluster administrator's own password for it to be compatible with the hash function (MD5) that is supported by the earlier release.

ONTAP accepts pre-hashed SHA-2 passwords only by using NetApp Manageability SDK (security-login-create and security-login-modify-password).

Manageability enhancements

1. Migrate the MD5 administrator accounts to the SHA-512 password hash function:
 - a. Expire all MD5 administrator accounts: `security login expire-password -vserver * -username * -hash-function md5`

Doing so forces MD5 account users to change their passwords upon next login.
 - b. Ask users of MD5 accounts to log in through a console or SSH session.

The system detects that the accounts are expired and prompts users to change their passwords. SHA-512 is used by default for the changed passwords.
2. For MD5 accounts whose users do not log in to change their passwords within a period of time, force the account migration:
 - a. Lock accounts that still use the MD5 hash function (advanced privilege level): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

After the number of days specified by -lock-after, users cannot access their MD5 accounts.

- b. Unlock the accounts when the users are ready to change their passwords: `security login unlock -vserver vservice_name -username user_name`
- c. Have users log in to their accounts through a console or SSH session and change their passwords when the system prompts them to do so.

When you need to update the Disk Qualification Package

The Disk Qualification Package (DQP) adds full support for newly qualified drives. Before you update drive firmware or add new drive types or sizes to a cluster, you must update the DQP. A best practice is to also update the DQP regularly; for example, every quarter or semi-annually.

You need to download and install the DQP in the following situations:

- Whenever you add a new drive type or size to the node

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
- Whenever you upgrade to a new version of ONTAP.

The DQP is not updated as part of an ONTAP upgrade.

Related information

[NetApp Downloads: Disk Qualification Package](#)

[NetApp Downloads: Disk Drive Firmware](#)

Copyright Information

Copyright © 2021 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.