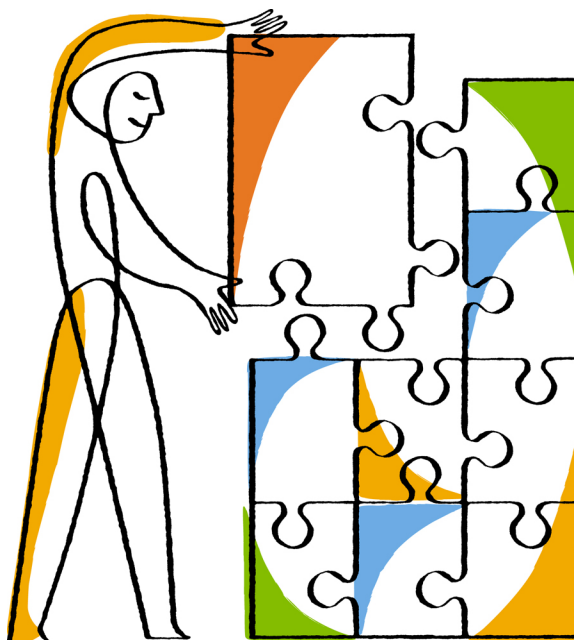




Updated for 8.2.1

Clustered Data ONTAP® 8.2

Upgrade and Revert/Downgrade Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-08519_C0
July 2014

Contents

Upgrading Data ONTAP clusters	8
Planning an upgrade to a Data ONTAP-v system	8
Planning your upgrade with Upgrade Advisor	9
Planning your upgrade	10
Types of cluster upgrades	11
Cluster upgrade checklist	11
Cluster upgrade requirements	17
Cluster upgrade limits	18
Required upgrade sequence for a batch upgrade	19
Guidelines for estimating the duration of the upgrade process	22
Upgrade considerations for an Infinite Volume	22
Upgrade requirements for SnapMirror	23
Information about low-memory V-Series system upgrade	24
Identifying potential upgrade issues	24
Preparing for the Data ONTAP cluster upgrade	28
Verifying the HA pair configuration	28
Verifying that deduplicated volumes and aggregates contain sufficient free space	29
Creating a performance baseline with Perfstat Converged	30
Verifying that the cluster is in quorum	31
Verifying cluster and SVM health	33
Enabling and reverting LIFs to home ports	34
Verifying the LIF failover configuration	36
Disabling automatic LIF rebalancing	37
Identifying active CIFS sessions that should be terminated	38
Verifying the system time	40
Determining the current software version on each node	41
Obtaining Data ONTAP software images	41
Installing Data ONTAP software images in a cluster	42
How Data ONTAP software images are stored and alternated in the cluster	43

Preparing SnapMirror relationships for a nondisruptive upgrade or downgrade	45
Ensuring that no jobs are running	46
Performing the software upgrade	47
Verifying that the cluster is ready to be upgraded	48
Upgrading a Data ONTAP cluster nondisruptively by using the rolling upgrade method	49
Upgrading a Data ONTAP cluster nondisruptively by using the batch method	61
Upgrading a Data ONTAP cluster disruptively	74
Completing post-upgrade tasks for cluster upgrades	76
Verifying the cluster version	76
Verifying that the cluster is in quorum	76
Verifying cluster and SVM health	78
Enabling and reverting LIFs to home ports	80
Creating a namespace mirror constituent for an upgraded Infinite Volume	81
Setting the cluster management LIF for Remote Support Agent	83
Resuming SnapMirror operations	84
Upgrading older style data protection mirror relationships	84
Enabling automatic LIF rebalancing	86
Updating firmware	87
How system firmware is updated during the Data ONTAP upgrade	87
Disk firmware updates	87
How disk firmware is updated	87
When you need to update the Disk Qualification Package	88
Service availability during disk firmware updates	89
Disk shelf firmware updates	90
How disk shelf firmware is updated	90
Detecting outdated disk shelf firmware	91
How ACP firmware is updated	91
Service Processor firmware updates	92
RLM firmware updates	92
How Flash Cache firmware is updated	92
Reverting clusters to an earlier Data ONTAP release family	94
When to revert and when to call technical support	94

Planning your reversion	95
Cluster reversion checklist	95
Reversion process considerations	98
Identifying potential reversion issues	99
Preparing to revert Data ONTAP clusters	100
Verifying that the cluster is in quorum	100
Verifying cluster and SVM health	102
Preparing to revert production clusters	104
Verifying the system time	118
Preparing Snapshot copies before reverting	119
Obtaining Data ONTAP software images	121
Installing Data ONTAP software images in a cluster	121
Reverting a Data ONTAP cluster	123
Completing post-reversion tasks	126
Verifying that the cluster is in quorum	126
Verifying cluster and SVM health	128
Enabling and reverting LIFs to home ports	129
Preparing Snapshot copies after reverting	131
Verifying client access (CIFS and NFS)	131
Considerations for downgrading the SP firmware	132
Reinstalling the required V-Series license after revert or downgrade	132
Enabling capability for SVM administrator with vsadmin role	133
Downgrading clusters to an earlier release in the same release family	134
When to downgrade and when to call technical support	134
Planning your downgrade	134
Cluster downgrade checklist	135
What to check before downgrading V-Series systems	138
Storage Encryption downgrade restriction	138
Downgrade process considerations	138
Identifying downgrade issues	139
Preparing for the Data ONTAP downgrade process	139
Verifying that the cluster is in quorum	139
Verifying cluster and SVM health	141
Enabling and reverting LIFs to home ports	143
Identifying active CIFS sessions that should be terminated	144

Verifying the system time	145
Checking for back-end configuration errors	146
Determining the current software version on each node before downgrading	147
Obtaining Data ONTAP software images	148
Installing Data ONTAP software images in a cluster	148
Preparing SnapMirror relationships for a nondisruptive upgrade or downgrade	150
Ensuring that no jobs are running	151
Performing the Data ONTAP downgrade process	152
Downgrading a Data ONTAP cluster nondisruptively	153
Downgrading a Data ONTAP cluster disruptively	157
Completing post-downgrade tasks	159
Verifying that the cluster is in quorum	159
Verifying cluster and SVM health	161
Enabling and reverting LIFs to home ports	163
Verifying client access (CIFS and NFS)	164
Resuming SnapMirror operations	164
Considerations for downgrading the SP firmware	165
Reinstalling the required V-Series license after revert or downgrade	165
Optimal service availability during upgrades	167
How upgrades impact service availability	167
Considerations for services and protocols during upgrades	167
Considerations for stateless protocols	168
Considerations for session-oriented protocols	168
Understanding background disk firmware updates	169
Upgrading Data ONTAP-v systems	170
Upgrade process overview for Data ONTAP-v systems	170
Recommendations for Data ONTAP-v systems upgrading to this release .	171
Preparing for a Data ONTAP-v system upgrade	171
Obtaining software images for Data ONTAP-v systems	172
Copying the software image to the HTTP server	172
Copying the software image from the HTTP server to the storage system .	173
Installing software images on Data ONTAP-v systems	173
Installing software images	174
Verifying Data ONTAP-v system status after an upgrade	174

Copyright information 176
Trademark information 177
How to send your comments 178
Index 179

Upgrading Data ONTAP clusters

Upgrading a cluster to the current Data ONTAP release requires preparation, the upgrade itself, and several post-upgrade procedures.

Note: It is a best practice to use Upgrade Advisor to plan your upgrade. Nonetheless, you might find useful detail and related information in this guide that complements your Upgrade Advisor plan.

If you are not able to use Upgrade Advisor, you should create your own upgrade plan manually by using guidelines provided in this guide.

The upgrade process includes the following phases:

- Preparing for the upgrade
- Performing the upgrade
- Completing post-upgrade tasks

Plan to do the following:

- Read the *Release Notes* for the target Data ONTAP release.
- Verify that all components of your configuration are compatible with the upgraded Data ONTAP release by consulting the Interoperability Matrix on the NetApp Support Site.

Unless otherwise indicated, the requirements and procedures in this guide apply to all supported:

- Data ONTAP 8.2.x platforms
For more information about supported platforms, see the *Release Notes* for the target Data ONTAP release.
- Upgrade paths to and within the Data ONTAP 8.2 release family
The supported upgrade paths include upgrades to releases in the Data ONTAP 8.2 release family from any 8.1.x release (*major upgrades*) and upgrades from 8.2.x to 8.2.z (*minor upgrades*).

Related information

NetApp Interoperability Matrix: support.netapp.com/NOW/products/interoperability

Planning an upgrade to a Data ONTAP-v system

Platforms that are based on Data ONTAP-v technology, such as Data ONTAP Edge systems, run standard Data ONTAP software and are upgraded in the same manner as other platforms. However, you should verify the versions of the hypervisor and related software before performing an upgrade.

For complete instructions, refer to the section for upgrading Data ONTAP-v systems and to the *Data ONTAP-v Administration Tool Installation Guide*.

Related concepts

[Upgrading Data ONTAP-v systems](#) on page 170

Planning your upgrade with Upgrade Advisor

You should use the Upgrade Advisor tool (if it is available in your environment) to ensure that you have met the requirements for upgrading to the current release and to generate an upgrade plan.

Before you begin

To use the Upgrade Advisor tool, your cluster must meet the following requirements:

- It must have a valid support contract.
- It must be enabled to send AutoSupport messages to NetApp.

Attention: If your cluster does not meet these requirements, you should consult the *Release Notes* and *Upgrade Guide* for this Data ONTAP release to prepare a detailed upgrade plan.

About this task

Upgrade Advisor is an online tool, available on the NetApp Support Site, that simplifies the process of planning Data ONTAP upgrades. When you submit your system identification and target release to Upgrade Advisor, the tool compares AutoSupport data about your cluster to known requirements and limitations of the target release. Upgrade Advisor then generates an upgrade plan (and optionally a back-out plan) with recommended preparation and execution procedures.

To generate an upgrade plan, you must have identifying information for your cluster (host name, system ID, or serial number) and you must have selected a target upgrade release. You can also select other options, including the following:

- Create a plan for a cluster.
- Create a back-out plan.
- Compare upgrade scenarios.

For more information about Upgrade Advisor, see the Upgrade Advisor Help screens.

Steps

1. Locate and record the system host name, system ID, or serial number of your cluster by entering the following command at the cluster shell:

```
system node run -node nodename sysconfig
```

The system identification information is near the top of the display.

2. From a web browser, log in to the My AutoSupport home page on the NetApp Support Site at the following URL: support.netapp.com/NOW/asuphome
3. Click the **Launch My AutoSupport** link.

10 | Upgrade and Revert/Downgrade Guide

4. Enter the host name, system ID, or serial number of your cluster when prompted.
5. Select the cluster that you want to upgrade from those listed.
6. Select the latest AutoSupport record from the ASUPs row.
7. Click the **Upgrade Advisor** tab.
8. Select the Data ONTAP release to which you want to upgrade from the **Target Versions** menu.
9. Select the upgrade method and the level of detail you want included in your upgrade plan.
10. Click **Continue** to generate your upgrade plan.

After you finish

It is not necessary to follow further instructions in this *Upgrade Guide* after you generate and execute an upgrade plan by using Upgrade Advisor. Nonetheless, you might want to consult this guide for details and background information.

Related information

Upgrade Advisor: support.netapp.com/NOW/asuphome

Planning your upgrade

Because new features are introduced in each release of Data ONTAP, you must understand these features and their associated upgrade requirements to evaluate how they might impact your current configuration. You are more likely to encounter issues if you are upgrading from a release earlier than the immediately previous version of Data ONTAP.

Note: It is a best practice to use Upgrade Advisor to plan your upgrade. Nonetheless, you might find useful detail and related information in this guide that complements your Upgrade Advisor plan.

If you are not able to use Upgrade Advisor, you should create your own upgrade plan manually by using guidelines provided in this guide.

Before proceeding with the upgrade, you should plan to do the following:

- Review the *Release Notes* for your Data ONTAP upgrade target release.
- Understand any requirements for upgrading to the target release from your existing software.
- Note any potential behavior changes to your cluster after the upgrade.
- Prepare to address all points in the upgrade checklist.
- Create a back-out plan, in the unlikely event that you need to revert or downgrade to the Data ONTAP release that was running on your cluster before the upgrade.

Unless otherwise indicated, the requirements and procedures in this guide apply to all supported Data ONTAP 8.2.x platforms. For more information about supported platforms, see the *Release Notes* for this Data ONTAP release.

Related concepts

[Reverting clusters to an earlier Data ONTAP release family](#) on page 94

[Downgrading clusters to an earlier release in the same release family](#) on page 134

Types of cluster upgrades

Based on your requirements, you can upgrade a cluster to a new Data ONTAP release by performing a nondisruptive upgrade or a disruptive upgrade.

In a *nondisruptive upgrade* (NDU), the cluster remains online and continues to serve data during the upgrade. There are two methods for performing a NDU:

- **Rolling upgrade**
In this method, a node is taken offline and upgraded while its partner takes over its storage. When the node upgrade is complete, the assisting partner gives control back to the original partner and the process is repeated, this time on the partner. Each additional HA pair is upgraded in sequence until all pairs are running the target release.
You can use this method for a cluster of any size, but it is required for clusters consisting of 2-6 nodes.
- **Batch upgrade**
In this method, the cluster is separated into two batches, each of which contains multiple HA pairs. In the first batch, one node in each HA pair is taken offline and upgraded while their partners take over their storage. When the upgrade is completed for the first half of all of the HA pairs, their partners give control back to them, and the process is repeated, this time on the partners. The process is then repeated on the second batch.
You can only use this method if the cluster consists of 8 or more nodes, and if it is configured for network-attached storage (NAS) only.

In a *disruptive upgrade*, the cluster is taken offline to perform the upgrade. This type of upgrade involves disabling storage failover for each HA pair and then rebooting each node.

You can perform a disruptive upgrade on a cluster of any size.

Cluster upgrade checklist

You can use this checklist to record your progress as you prepare for the upgrade, perform the upgrade, and complete post-upgrade tasks.

Steps for preparing to upgrade

Preparatory steps are complete when all of the following conditions are true:

Condition	Complete?
Software and hardware support in the target release is confirmed. To confirm hardware support, visit <i>Hardware Universe</i> at hww.netapp.com	

Condition	Complete?
<p>Cluster network and management network switches are supported.</p> <p>The software, firmware, and reference configuration files used by cluster and management Ethernet switches must be compatible with Data ONTAP. When planning a Data ONTAP deployment or upgrade, you must consult the <i>Cluster and Management Ethernet Switch Matrix</i> to determine whether updates are also required to the switch configurations.</p>	
<p>The SAN configuration is fully supported.</p> <p>All SAN components—including target Data ONTAP software version, host OS and patches, required Host Utilities software, and adapter drivers and firmware—should be listed in the <i>NetApp Interoperability Matrix</i> on the NetApp Support Site.</p>	
All release-specific upgrade issues have been resolved.	
You have clustershell access privileges.	
<p>You have created a performance baseline.</p> <p>You use Perfstat Converged to create a performance baseline.</p>	
<p>A remote management device is configured for each node.</p> <p>You should have either a Service Processor (SP) or Remote LAN Module (RLM) device configured. For more information, see the <i>Clustered Data ONTAP System Administration Guide for Cluster Administrators</i>.</p>	
<p>The HA pair is verified.</p> <p>You can use the Config Advisor tool to check for common configuration errors.</p>	
<p>Deduplicated volumes and aggregates contain sufficient free space.</p> <p>Each deduplicated volume must contain at least 4% free space.</p> <p>Each aggregate that contains a deduplicated volume must contain at least 3% free space.</p>	
<p>The cluster is in quorum.</p> <p>Ensure that all nodes are participating in a quorum and all rings are in the quorum. Verify also that the per-ring quorum master is the same for all nodes.</p>	

Condition	Complete?
<p>The cluster and Storage Virtual Machines (SVMs) are running and healthy.</p> <p>All aggregates and volumes should be healthy and online before proceeding with the upgrade. You can use the <code>cluster show</code> command to verify the status of the nodes.</p>	
<p>LIFs are online and on their correct home ports.</p> <p>You can use the <code>network interface</code> command to display and modify LIF configuration.</p>	
<p>The LIF failover configuration is verified.</p> <p>Each data LIF must have the correct failover policy, failover group, and failover targets applied.</p>	
Automatic LIF rebalancing is disabled (for batch upgrades only).	
Any CIFS sessions that are not continuously available have been terminated.	
The system time is synchronized across the cluster.	
<p>Each node is running Data ONTAP 8.1 or later.</p> <p>Ensure that you are running on the minimum software version allowed for the upgrade by running the <code>system node image show</code> command.</p>	
<p>You have the target Data ONTAP software image available on an HTTP or FTP server.</p> <p>Download the software image for the target Data ONTAP release from the NetApp Support Site at support.netapp.com, and place it on an HTTP or FTP server that is accessible by each node.</p>	
<p>The target Data ONTAP software images are installed on each node and set as the alternate boot device image.</p> <p>You can use the <code>system node image update</code> command to install the software images. You can use the <code>system node image show</code> command to verify that the software images are installed as the alternate boot image on each node.</p>	
SnapMirror operations are suspended.	

Condition	Complete?
No jobs are running. If any aggregate, volume, mirror, NDMP (dump or restore), or Snapshot jobs (such as create, delete, move, modify, replicate, and mount jobs) are running or queued, allow the jobs to complete successfully or stop the queued entries.	

Steps for performing a rolling upgrade

If you are performing a nondisruptive upgrade by using the rolling upgrade method, the upgrade is complete when all of the following steps have been completed:

Condition		Complete?
You have verified that the cluster is ready to be upgraded nondisruptively.		
The first HA pair is upgraded.	The first node in the HA pair is upgraded.	
	The node's partner is upgraded.	
	You have verified that the HA pair was upgraded successfully.	
If needed, the second HA pair is upgraded.	The first node in the HA pair is upgraded.	
	The node's partner is upgraded.	
	You have verified that the HA pair was upgraded successfully.	
If needed, the third HA pair is upgraded.	The first node in the HA pair is upgraded.	
	The node's partner is upgraded.	
	You have verified that the HA pair was upgraded successfully.	
You have verified that the cluster upgrade was completed successfully.		

Steps for performing a batch upgrade

If you are performing a nondisruptive upgrade by using the batch upgrade method, the upgrade is complete when all of the following steps have been completed:

Condition	Complete?
You have verified that the cluster is ready to be upgraded nondisruptively.	

Condition		Complete?
The cluster is divided into two batches. If the cluster has an even number of HA pairs, then each batch should contain half of the HA pairs. If the cluster has an odd number of HA pairs, then the first batch should contain one more HA pair than the second batch.		
The first batch is upgraded.	The first node in each HA pair is upgraded.	
	The nodes' partners are upgraded.	
	You have verified that the HA pairs were upgraded successfully.	
The second batch is upgraded.	The first node in each HA pair is upgraded.	
	The nodes' partners are upgraded.	
	You have verified that the HA pairs were upgraded successfully.	
You have verified that the cluster upgrade was completed successfully.		

Steps for performing a disruptive upgrade

If you are performing a disruptive upgrade, the upgrade is complete when all of the following steps have been completed:

Condition	Complete?
You have verified that the cluster is ready to be upgraded disruptively.	
Storage failover is disabled and each node is rebooted.	
You have verified that the cluster upgrade was completed successfully.	

Steps for after upgrading

Post-upgrade steps are complete when all of the following conditions are true:

Condition	Complete?
The cluster and SVMs are running and healthy. All aggregates and volumes should be healthy and online before proceeding with the upgrade. You can use the <code>cluster show</code> command to verify the status of the nodes.	

Condition	Complete?
LIFs are online and on their correct home ports. You can use the <code>network interface</code> command to display and modify LIF configuration.	
A namespace mirror constituent exists for an Infinite Volume. If the cluster contains an Infinite Volume that spans two or more nodes, you must create a namespace mirror constituent to provide data protection for the namespace constituent.	
The cluster management LIF is set correctly for Remote Support Agent. You can set the cluster management LIF by using the <code>rsa setup</code> command on each SP or RLM device.	
SnapMirror operations are resumed. If you suspended SnapMirror operations prior to performing a nondisruptive upgrade, you should resume the operations after the upgrade is complete.	
Older style data protection mirror relationships are updated. SnapMirror relationships that you have before upgrading to Data ONTAP 8.2 must use the Data ONTAP 8.2 syntax style if you want to make use of its features and improvements.	
Automatic LIF rebalancing is reenabled.	

Related concepts

Identifying potential upgrade issues on page 24

Performing the software upgrade on page 47

Related tasks

Preparing for the Data ONTAP cluster upgrade on page 28

Completing post-upgrade tasks for cluster upgrades on page 76

Related information

Cluster and Management Ethernet Switch Support Matrix: support.netapp.com/NOW/download/software/cm_switches

NetApp Interoperability Matrix: support.netapp.com/NOW/products/interoperability

Cluster upgrade requirements

There are release and configuration requirements that your cluster should meet before you perform an upgrade. Additionally, there are mixed version requirements that you should be aware of while you are performing the upgrade.

Release requirements

You can upgrade clusters to the Data ONTAP 8.2 release family from any 8.1.x release. Minor upgrades within the Data ONTAP 8.2 release family are supported from all previous 8.2 releases.

Note: If you are running Data ONTAP GX 10.x, do not attempt to upgrade clusters to the Data ONTAP 8.2 release family on your own; doing so is an unsupported operation. Contact your NetApp representative for assistance.

If you want to upgrade to a Data ONTAP 8.2 release from a release earlier than 8.1, you must perform an intermediate upgrade (also known as a multi-hop upgrade) to the latest Data ONTAP 8.1 release before upgrading to the target Data ONTAP 8.2 release.

Configuration requirements

The cluster must meet the following configuration requirements before you upgrade it:

- Because failed disk drives prevent giveback operations and can introduce loop instability throughout the cluster, you must remove or replace all failed disk drives *before* beginning the upgrade process.
For more information about identifying and removing failed disks, see the *Clustered Data ONTAP Physical Storage Management Guide*.
- If your cluster serves NFS clients, you must use hard mounts.
You should not use soft mounts when there is a possibility of frequent NFS timeouts, which can lead to disruptions during the upgrade process and possible data corruption.
- If your cluster serves CIFS clients, nondisruptive upgrades are supported for Hyper-V over SMB solutions.
Hyper-V over SMB solutions enable Hyper-V and the contained virtual machines to remain online and to provide continuous availability during the Data ONTAP upgrade. For more information and configuration limits and requirements, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.
For all other CIFS configurations, client sessions are terminated. You should direct users to end their sessions before you upgrade to prevent data loss.
- Upgrades might be disruptive if the cluster is actively serving Network Data Management Protocol (NDMP) clients that cannot be postponed.
Because this protocol is session-oriented, current sessions must finish, and the service must be disabled to use nondisruptive upgrades.

Mixed version requirements

Data ONTAP clusters can operate for a limited time in a *mixed version* state, in which nodes in a cluster are running Data ONTAP versions from different release families. However, the upgrade is not complete until all nodes are running the new target release.

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

Related tasks

Creating a performance baseline with Perfstat Converged on page 30

Cluster upgrade limits

Before performing an upgrade, you must verify that your cluster does not exceed the platform system limits. SAN and Hyper-V over SMB also have limits that you should verify in addition to the platform system limits.

General platform limits

You should not exceed the system limits for your platform. To obtain your platform's system limits, see the *Hardware Universe* at hww.netapp.com. In addition, you should not exceed the maximum values for the following system elements:

Element	Value (per node)	Command to display values
Snapshot copies	20,000	<code>volume snapshot show</code>
CPU utilization *	No greater than 50%	<code>node run -node node_name - command sysstat -c 10 -x 3</code>
Disk utilization *	No greater than 50%	

* Before upgrading Data ONTAP, 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 ten measurements reported. You should ensure that no additional load is added to the cluster until the upgrade completes.

Note: You should use the Performance and Statistics Collector (Perfstat Converged) tool to establish a performance baseline for comparison with performance after the upgrade.

SAN limits

If your cluster is configured for SAN, you should not exceed the limits defined in the *Clustered Data ONTAP SAN Configuration Guide*.

Hyper-V over SMB limits

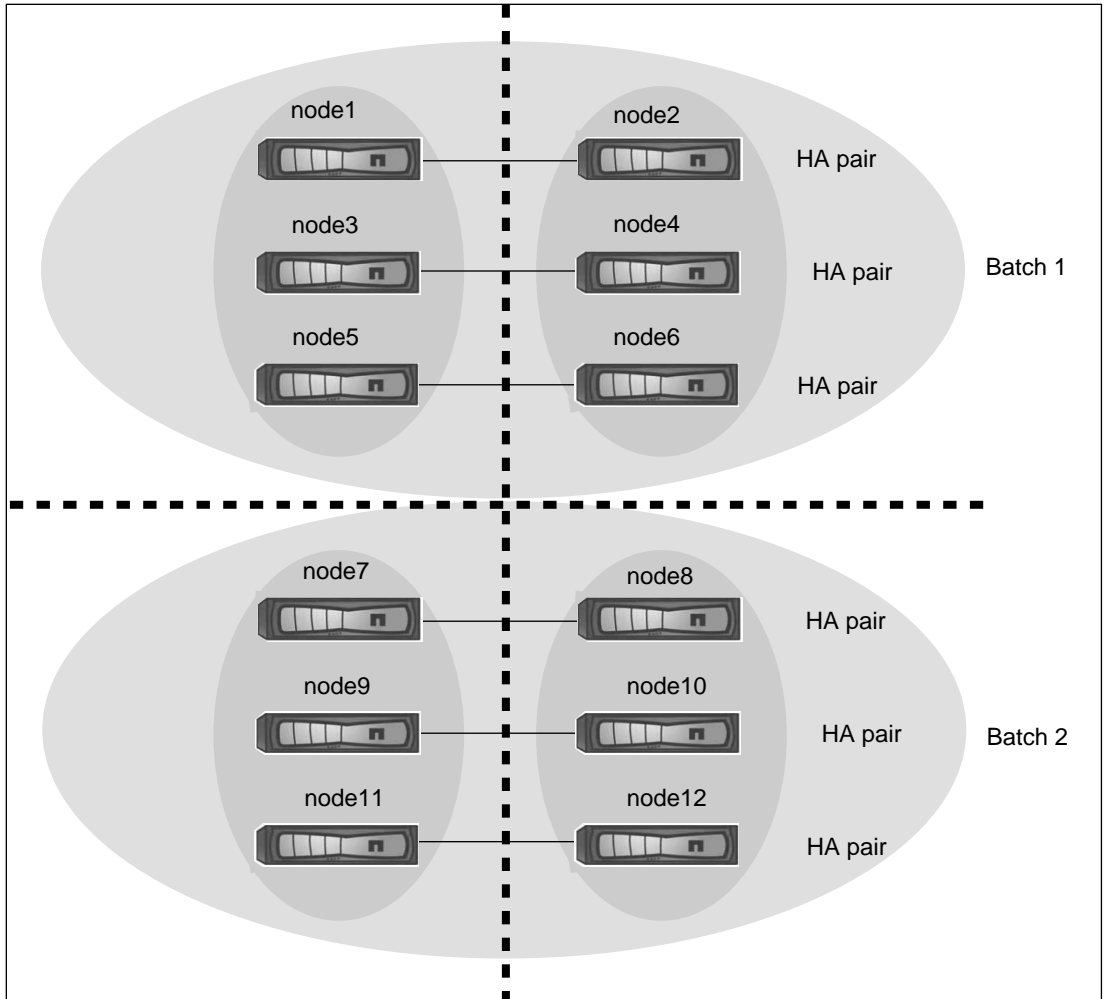
If you have configured a Hyper-V over SMB solution, you should not exceed the maximum values for the following system elements on all platforms:

Element	Value (per node)	Command to display values
FlexVol volumes	200	<code>volume show -node <i>node_name</i></code>
LUNs	400	<code>lun show</code>
Snapshot copies	2,000	<code>volume snapshot show</code>

Required upgrade sequence for a batch upgrade

Performing a batch upgrade requires you to upgrade sets of nodes in a particular sequence. By following the required sequence, you can ensure that the cluster will remain up and continue serving data while you perform the NDU.

The following diagram illustrates the batch upgrade sequence for a 12-node cluster:

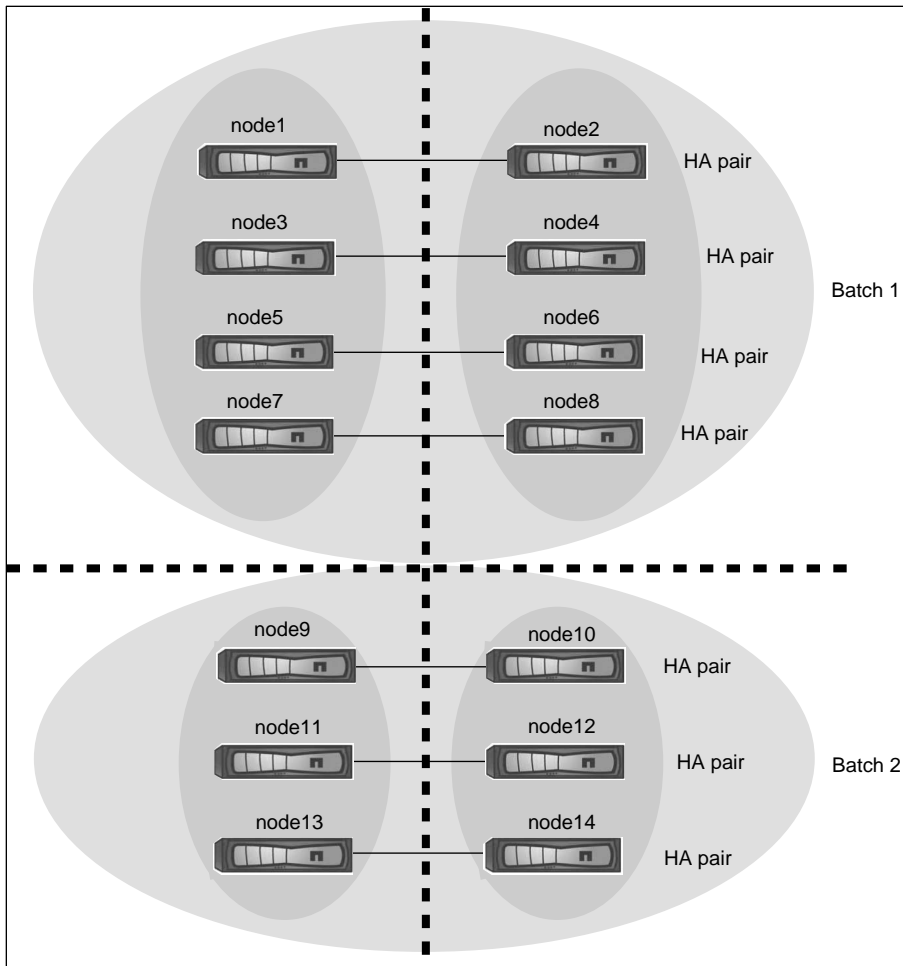


Note: The node names in this diagram are provided for example purposes only. The nodes are numbered to depict the proper upgrade sequence.

This cluster is divided into two batches, each containing an equal number of HA pairs. The nodes are then upgraded in the following sequence:

1. Batch 1:
 - a. Upgrade node1, node3, and node5 concurrently
 - b. Upgrade node2, node4, and node6 concurrently
2. Batch 2:
 - a. Upgrade node7, node9, and node11 concurrently
 - b. Upgrade node8, node10, and node12 concurrently

If a cluster contains an odd number of HA pairs, the first batch should contain the larger number of HA pairs. For example, the following diagram shows the batch upgrade sequence for a 14-node cluster, in which the first batch contains 4 HA pairs, and the second batch contains 3 HA pairs:



In this 14-node cluster, the nodes are upgraded in the following sequence:

1. Batch 1:
 - a. Upgrade node1, node3, node5, and node7 concurrently
 - b. Upgrade node2, node4, node6, and node8 concurrently
2. Batch 2:
 - a. Upgrade node9, node11, and node13 concurrently
 - b. Upgrade node10, node12, and node14 concurrently

Guidelines for estimating the duration of the upgrade process

For each HA pair, you should plan for approximately 30 minutes to complete preparatory steps, 60 minutes to perform the upgrade, and 30 minutes to complete post-upgrade steps.

The batch method for performing a nondisruptive upgrade enables you to upgrade all of the HA pairs in a batch concurrently. Accordingly, if you perform a batch upgrade, the total amount of time required to upgrade the cluster should be similar to the amount of time required to upgrade two HA pairs regardless of the size of the cluster.

The 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.

Upgrade considerations for an Infinite Volume

When upgrading a cluster that is running Data ONTAP 8.1.1 or later, and the cluster contains an Infinite Volume, you must understand the order of upgrading the nodes and the procedures you must perform after the upgrade.

If technical support created a data protection mirror copy for the namespace constituent in an Infinite Volume running Data ONTAP 8.1.x, you should upgrade the node with the data protection mirror copy for the namespace constituent first. If technical support did not create a data protection mirror copy for the namespace constituent, you can upgrade the nodes in any order.

After the upgrade, Infinite Volumes that span two or more nodes must have a namespace mirror constituent to provide data protection for the Infinite Volume's namespace constituent. The upgrade process does not automatically create the namespace mirror constituent. You must review the post-upgrade procedure for Infinite Volumes and plan for how to create a namespace mirror constituent after the upgrade.

After the upgrade, Infinite Volumes that are in a data protection mirror relationship must use Storage Virtual Machine (SVM) peering between the SVM with Infinite Volume in the source cluster and the SVM with Infinite Volume in the destination cluster to enable the data protection features available in Data ONTAP 8.2.x. The upgrade process does not automatically configure SVM peering or the new relationship capabilities. You must review the post-upgrade procedure and plan for how to upgrade the data protection mirror relationship to use SVM peering and the new relationship capabilities after the upgrade.

Related tasks

[*Creating a namespace mirror constituent for an upgraded Infinite Volume*](#) on page 81

[*Upgrading older style data protection mirror relationships*](#) on page 84

Upgrade requirements for SnapMirror

Before upgrading a cluster that is running SnapMirror, SnapMirror operations must be suspended 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 a Data 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 (non-disruptive 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 you are performing a batch upgrade or 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. This option requires you to perform a rolling upgrade; batch upgrades are not permitted.	Yes.

SVM peering requires SVM names to be unique across clusters. You should 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.

For more information about running SnapMirror on clusters configured for network-attached storage (NAS), see the *Clustered Data ONTAP Data Protection Guide*.

Information about low-memory V-Series system upgrade

While upgrading your low-memory V-Series system (a storage system with physical memory of 8 GB or less; for example V3140, V3160, V3210, and V3240) from a previous Data ONTAP release to Data ONTAP 8.2.1, your system might undergo multiple reboots.

Multiple reboots occur if the number of storage devices discovered by the V-Series system exceeds the maximum number of storage devices allowed for that platform. This happens because, in Data ONTAP 8.2.1, memory is allocated dynamically for storage devices as you present the storage devices to your V-Series system.

For information about the number of storage devices allowed for different platforms, see the *Hardware Universe* at hww.netapp.com.

Note: The term V-Series system refers to the storage systems released prior to Data ONTAP 8.2.1 that can use array LUNs. The FAS systems released in Data ONTAP 8.2.1 and later can use array LUNs if the required license is installed.

Identifying potential upgrade issues

Every Data ONTAP release family has unique upgrade requirements that you must understand before you decide to upgrade.

Before you upgrade, you must understand the following:

- Issues you must resolve before upgrading to the new release
- New system behavior after upgrading to the new release

Because significant new features are introduced in each new Data ONTAP release family, you might encounter issues when upgrading to a new release family.

Be sure to consult the *Release Notes* for the upgrade target release for a complete listing of upgrade issues.

Upgrade issues with the Data ONTAP 8.2 release family

You must understand and resolve any known technical issues before you upgrade a cluster to Data ONTAP 8.2 and later releases.

This topic summarizes significant issues known at publication time. Be sure to check the "Important Cautions" section in the latest *Release Notes* for your target Data ONTAP release to see a complete list of issues that could affect the upgrade.

- Starting with Data ONTAP 8.2.1, there is a change in how Data ONTAP handles file names containing UTF-16 supplementary characters that you must be aware of if your environment uses such file names.
- After you upgrade to Data ONTAP 8.2, the license-list-info ZAPI is no longer supported. As a result, you must install Data ONTAP management software versions that are supported by Data ONTAP 8.2 or later.
- During a Data ONTAP upgrade, LUNs are assigned new revision numbers. Windows Server 2008 and Windows Server 2012 interpret the LUNs with new revision numbers as new disks and set them offline after a host reboot; this status is shown in Windows management interfaces after the upgrade. Windows Server 2003 ignores LUN revision numbers.
- Stale deduplication-related metadata can exist in the FlexVol volumes and aggregates on your system, resulting in slow deduplication processing or your systems running out of space. Your systems can experience this problem if you are upgrading from a Data ONTAP 8.1 release prior to 8.1.2P4, if deduplication is enabled on any FlexVol volume, and if a FlexVol volume or the associated aggregate is more than 70 percent full.
- Starting with Data ONTAP 8.2, all license keys are 28 characters in length. Licenses installed prior to Data ONTAP 8.2 continue to work after you upgrade to Data ONTAP 8.2 or later. However, if you need to reinstall a license when you are running Data ONTAP 8.2 or later, the old key is not accepted.
- Starting with Data ONTAP 8.2, a baseline SP firmware image is packaged with the Data ONTAP image. By default, the SP automatic update functionality is enabled. You have the option to manually trigger an SP update.
- Starting with Data ONTAP 8.1.2, the software install or upgrade includes new disk shelf firmware versions for DS14mk2 AT and DS4243 disk shelves that provide enhanced disk error detection and prediction capabilities. Therefore, after upgrading to this version of Data ONTAP, you might experience an increase in the number of disk failures for certain disk shelf and disk models.
- Data ONTAP permits you to create multiple CIFS super user accounts for the same user if the domain name for each account is entered using a different format. This can lead to CIFS service outages after you upgrade from Data ONTAP 8.1.x to Data ONTAP 8.2.
- If you have a 3210 or 3140 system with Flash Cache modules installed, do not upgrade to clustered Data ONTAP 8.2 or later 8.2.x releases. Flash Cache modules are not supported on 3210 or 3140 systems running clustered Data ONTAP 8.2 or later 8.2.x releases.
- Starting with Data ONTAP 8.2.1, the off-board antivirus feature is supported. To enable the off-board antivirus feature, you must ensure that all the nodes in the cluster are running Data ONTAP 8.2.1 or later.
- Beginning with Data ONTAP 8.2, striped volumes are no longer supported. You should not upgrade to Data ONTAP 8.2 if there are striped volumes in your environment.
- Beginning with Data ONTAP 8.2, NFSv2 is no longer supported and all NFSv2 functionality has been removed from Data ONTAP.

If you still require the use of the NFSv2 protocol in your environment, do not upgrade to Data ONTAP 8.2 or later until you have discontinued use of NFSv2.

- If you have a `flex_clone` license, you must turn on the `licensed_feature.flex_clone` option after you upgrade to Data ONTAP 8.2.
- In Data ONTAP 8.2.x releases, you must ensure that there is sufficient space on the aggregate and on the volume to upgrade the deduplication metadata.
You can use the `df` command to check the space available on the aggregate and on the volume.
- Modifying certain 7-Mode CIFS-specific options to a non-default value on a controller running clustered Data ONTAP 8.1.x or 8.2.x and then upgrading to a later version of 8.2.x might lead to recursive service disruptions.
- Starting with Data ONTAP 8.1.3, support for on-board antivirus is discontinued.
Therefore, you must disable on-board antivirus and unschedule all the antivirus on-demand (AVOD) jobs before upgrading to Data ONTAP 8.2 and later.
- Beginning with Data ONTAP 8.2.1, Data ONTAP now sends DNS queries to resolve domain names in export policy rules by default over the data LIF, not the node management LIF.
- Beginning with Data ONTAP 8.2.1, Data ONTAP now sends DNS queries to resolve host names in export policy rules by default over the data LIF, not the node management LIF.
- Exceeding recommended maximums on CIFS servers might lead to a disruption of service.
You should not exceed recommended maximums on the number of CIFS local users and groups that you can create on the cluster.
- When NFSv3 or NFSv4.x clients attempt to modify file attributes using a `chmod`, `chown`, or `chgrp` command for a path that represents a junction point on volumes with UNIX security style, the operation appears successful but actually fails silently.
If the client attribute cache is enabled, it is populated with incorrect information.
- If you upgrade from a version of Data ONTAP that does not support SMB 3.0 to a version of Data ONTAP that does, reconnections to mapped SMB shares from Windows 8 or Windows 2012 Server might fail with an “Invalid Signature” error.
Data ONTAP 8.2 and later releases support SMB 3.0.
- Although Data ONTAP supports both the NFS and SMB file access protocols, file access over NFSv3 from Windows clients is currently only supported in Data ONTAP operating in 7-Mode; it is not supported in clustered Data ONTAP.
- If you want to use clustered Data ONTAP 8.2.1 with NFSv4.1 or pNFS in your environment with Red Hat Enterprise Linux (RHEL), you must ensure that your RHEL clients meet certain requirements.
- Under certain circumstances, high load on the storage system or DNS timeouts can result in access issues for NFS clients connecting over IPv6.

Changes to behavior in the Data ONTAP 8.2 release family

You should be aware of changes in Data ONTAP behavior that occur if you upgrade a cluster to Data ONTAP 8.2 or later.

This topic summarizes significant changes known at publication time. Be sure to check the *Known Problems and Limitations* section in the *Release Notes* for your target Data ONTAP release to see a complete list of changes in behavior after upgrade to the target release.

- Starting with Data ONTAP 8.2, the Network Time Protocol (NTP) is always enabled on the cluster.
If you manually set the time, the setting takes effect on all nodes in the cluster.
- Starting with Data ONTAP 8.2, switchless two-node clusters of FAS22xx systems can be configured using only a single 10-GbE port on each node for the cluster network.
- Starting with Data ONTAP 8.2, Element Manager (including ClusterView) is no longer available. You can use the Data ONTAP command-line interface or OnCommand System Manager, a web-based graphical management interface, to manage the cluster.
- Starting in Data ONTAP 8.2, aggregate Snapshot copy automatic deletion is always enabled and cannot be disabled.
- In previous versions of Data ONTAP, you could set the fractional reserve setting for a FlexVol volume to any value between 0 and 100, inclusive.
Starting with Data ONTAP 8.2, the fractional reserve setting can be set only to 0 or 100.
- Starting with Data ONTAP 8.2, Data ONTAP generates aliases based on SN instead of the WWN.
- In the node-scoped NDMP mode, you must use NDMP-specific credentials to access a storage system in order to perform tape backup and restore operations.
- Before using NFSv4.1 or pNFS on your storage system with NFS clients, you should take certain precautions to ensure successful deployment in your environment.
- When upgrading to Data ONTAP 8.2, the cluster can operate in a mixed-version state, in which some nodes are running release 8.2 and some are running release 8.1.
While in this state, the cluster switch health monitor might generate health alerts. These alerts trigger AutoSupport messages that include an incorrect subject.
- The default LDAP client schema AD-SFU that was provided by Data ONTAP 8.1 does not work with Windows Services for UNIX (SFU) or Identity Management for UNIX (IDMU).
During the upgrade to Data ONTAP 8.2, this problem is corrected.
- SnapMirror relationships that you had before upgrading to Data ONTAP 8.2 must use the Data ONTAP 8.2 syntax style if you want to make use of its features and improvements.
- For an intercluster Storage Virtual Machine (SVM) peer relationship that is in pending state, if the cluster administrator of the local cluster deletes the SVM peer relationship and the cluster administrator of the peer cluster accepts the SVM peer relationship simultaneously, then both the clusters might have an inconsistent state with respect to SVM peer relationship.
- Avoid configuring LIFs with addresses in the 192.168.1/24 and 192.168.2/24 subnets.
LIFs configured with these addresses may conflict with private iWARP interfaces and might result in the LIFs failing to come on line after a node reboot or a LIF migration.
- Fast path is enabled by default in all nodes in the cluster.
However, you might have to disable fast path in certain scenarios to avoid issues such as performance degradation or failed software upgrade.
- If you are configuring volumes with zero fractional reserve and you are using certain technologies or Data ONTAP features, you must take some extra precautions to avoid out of space errors.
- If you configure ACP to use a different port than e0P (the default) on FAS2240 systems, the internal ACPP module IOM6E becomes unresponsive, disabling ACP for the local SAS expander.

Unless you are experiencing hardware issues on port e0P, always use the default port for ACP for the FAS2240 systems.

- FlexCache volumes are not supported on the following FAS systems running clustered Data ONTAP 8.2: 3140, 3160, 3210, and 3240.
- Starting with Data ONTAP 8.2, the new NFS server parameter `-mount-rootonly` is enabled by default, meaning Data ONTAP by default now rejects all NFS mount requests from nonreserved ports (ports numbered 1024 or higher).

If your environment has clients that require mounting NFS exports using nonreserved ports, you must manually disable this parameter for each SVM after upgrading to Data ONTAP 8.2 or later.

Preparing for the Data ONTAP cluster upgrade

Before installing the latest Data ONTAP release on your cluster, you must perform several cluster health checks, including ensuring that the cluster is running and healthy, verifying that the cluster is in a quorum, and verifying the Storage Virtual Machine (SVM) health.

Verifying the HA pair configuration

You can go to the NetApp Support Site and download the Config Advisor tool to check for common configuration errors.

About this task

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

Note: Support for Config Advisor is limited, and available only online.

Steps

1. Log in to the NetApp Support Site at support.netapp.com and go to **Downloads > Utility ToolChest**.
2. Click **Config Advisor (WireGauge renamed)**.
3. Follow the directions on the web page for downloading, installing, and running the utility.
4. After running Config Advisor, review the tool's output and follow the recommendations to address any issues discovered.

Verifying that deduplicated volumes and aggregates contain sufficient free space

Before upgrading Data 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 Data ONTAP upgrade is completed.

About this task

Each deduplicated volume must contain at least 4% free space. Each aggregate that contains a deduplicated volume must contain at least 3% free space.

Steps

1. Determine which volumes are deduplicated:

```
volume show -is-sis-volume true
```

Example

This example displays a deduplicated volume and the aggregate that contains it.

```
cluster1::> volume show -is-sis-volume true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
vs1	vol_2	aggr_2	online	RW	20GB	18.74GB	6%

2. Determine the free space available on each volume that you identified:

```
df -vserver Vserver_name -volume volume_name
```

Each deduplicated volume must not contain more than 96% used capacity.

Example

In this example, the `capacity` field displays the percentage of used space on the deduplicated volume identified earlier (`vol_2`).

```
cluster1::> df -vserver vs2 -volume vol_2
```

Filesystem	kbytes	used	avail	capacity	Mounted on
/vol/vol_2/	19456000	264000	19192000	1%	/
/vol/vol_2/.snapshot	1024	0	1024	0%	//.snapshot

2 entries were displayed.

For details on how to increase the size of a volume, see the *Clustered Data ONTAP Logical Storage Management Guide*.

3. Identify the free space available on each aggregate that contains a deduplicated volume:

```
df -A -aggregate aggregate_name
```

Each aggregate must not contain more than 97% used capacity.

Example

In this example, the `capacity` field displays the percentage of used space on the aggregate containing the deduplicated volume (`aggr_2`).

```
cluster1::> df -A -aggregate aggr_2
Aggregate      kbytes      used      avail capacity
aggr_2          344220000    20944000    323276000    6%
aggr_2/.snapshot      0          0          0      0%
2 entries were displayed.
```

For details on how to increase the size of an aggregate, see the *Clustered Data ONTAP Physical Storage Management Guide*.

Creating a performance baseline with Perfstat Converged

The Performance and Statistics Collector (Perfstat Converged) is a cluster diagnostics data collection tool, available on the NetApp Support Site, that enables you to establish a performance baseline for comparison after the upgrade. You should create a Perfstat report before upgrading.

Before you begin

The `diag` user account must be unlocked. For details about unlocking this account, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

About this task

You should create a Perfstat report during a typical usage time; this takes about 30 minutes.

Steps

1. Download Perfstat Converged from the NetApp Support Site at support.netapp.com/NOW/download/tools/perfstat.
2. Enter the following command during a typical usage period:

```
perfstat8 cluster_management_IP_address -m c -t 4 -i 5 -z
```

After you finish

You should retain the output file for several weeks after the Data ONTAP upgrade is complete.

Verifying that the cluster is in quorum

Before and after you perform an upgrade, reversion, or downgrade, you must ensure that all nodes are participating in a replicated database (RDB) quorum and that all rings are in the quorum. You must also verify that the per-ring quorum master is the same for all nodes.

About this task

For more information about cluster replication rings and RDB quorums, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

1. Set the privilege level to advanced:
set -privilege advanced
Enter **y** to continue.
2. Display each RDB process:

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

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.1.x:

```
cluster1::*> cluster ring show -unitname vldb

Node   UnitName Epoch DB Epoch DB Trnxs Master
-----
node0  vldb     154   154      14847  node0
node1  vldb     154   154      14847  node0
node2  vldb     154   154      14847  node0
node3  vldb     154   154      14847  node0
4 entries were displayed.
```

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.2.x:

```
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.

```

For each process, verify the following configuration details:

- The relational database epoch and database epochs match for each node.
- The per-ring quorum master is the same for all nodes.

Note that each ring might have a different quorum master.

3. Return to the admin privilege level:

```
set -privilege admin
```

4. 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. During the upgrade, reversion, or downgrade process, each node will temporarily fall out of SAN quorum. Therefore, if you are verifying the SAN quorum after completing an upgrade, reversion, or downgrade, you may notice critical event messages warning you that the nodes were previously out of SAN quorum.

If a node is out of SAN quorum, you can use the `storage failover takeover` and `storage failover giveback` commands to perform a planned takeover and giveback with the node's high-availability partner and bring the node back into SAN quorum.

Example

In this example, both nodes in the cluster are in SAN quorum.

```

cluster1:>> event log show -messagename scsiblade.*
Time          Node      Severity      Event
-----
8/13/2013 14:03:51 node0      INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 14:03:51 node1      INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...

```

Example

This example shows a two-node cluster after performing an upgrade. Each node shows a previous out of SAN quorum event message from when the node was upgraded. However, the most recent event message for each node shows that both nodes are presently in SAN quorum.

```

cluster1:>> event log show -messagename scsiblade.*
Time          Node      Severity      Event
-----
8/13/2013 15:37:51 node1      INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:31:26 node1      CRITICAL      scsiblade.out.of.quorum: This node ...
8/13/2013 15:31:26 node1      INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:31:26 node1      INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:30:43 node0      INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:24:16 node0      CRITICAL      scsiblade.out.of.quorum: This node ...
8/13/2013 15:24:16 node0      INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:24:16 node0      INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...

```


Verifying cluster and SVM health

Before and after you upgrade, revert, or downgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and the aggregates and volumes are online.

Steps

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster:

```
cluster show
```

Example

```
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. For more information about EMS messages, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

To troubleshoot cluster health issues, see the knowledgebase article [Troubleshooting Workflow: RDB app out of quorum](#) on the NetApp Support Site.

2. Determine if any disk drives are broken, undergoing maintenance, or reconstructing:

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

3. To verify that all aggregates are online, display the state of physical and logical storage, including storage aggregates:

```
storage aggregate show -state !online
```

This command displays the aggregates that are *not* online.

Example

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

For more information about managing aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide*.

4. To verify that all volumes are online, display any volumes *not* online:

```
volume show -state !online
```

Example

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

For more information about managing volumes, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Enabling and reverting LIFs to home ports

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

About this task

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.

Steps

1. Display the status of all LIFs:

```
network interface show
```

Example

This example displays the status of all LIFs for a Storage Virtual Machine (SVM, formerly known as Vserver).

```
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
```

Example

```

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

```

3. Revert LIFs to their home ports:

```
network interface revert *
```

Example

This command reverts all LIFs back to their home ports and changes all LIF home statuses to true.

```

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

```

4. Verify that all LIFs are in their home ports:

```
network interface show
```

Example

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.

```


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 will first attempt to fail over to port e0c on node0. If lif0 cannot fail over to e0c, it will next attempt to fail over to port e0d on node0, and so on.

2. If the data ports are on different VLANs or subnets, verify for each LIF that the failover group is user-defined.

A user-defined failover group must be configured for each VLAN or broadcast domain, and each LIF must subscribe to the corresponding failover group. For more information about configuring LIF failover groups, see the *Clustered Data ONTAP Network Management Guide*.

3. If the failover policy is set to disabled for any of the LIFs, use the `network interface modify` command to enable failover.
4. 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 create` command to add a failover target to the failover group.

Disabling automatic LIF rebalancing

By disabling automatic LIF rebalancing before performing a batch upgrade, you can ensure that the LIFs remain online during the entire upgrade procedure.

About this task

When automatic LIF rebalancing is enabled, LIFs can be migrated to a less-utilized port on another node based on the LIF failover configuration. However, because a batch upgrade enables you to upgrade multiple nodes concurrently, automatic LIF rebalancing could cause the LIFs to migrate to a node that is rebooting.

Steps

1. Set the privilege level to advanced:
`set -privilege advanced`
2. View and record any LIFs that have automatic LIF rebalancing enabled:
`network interface show -allow-lb-migrate true`

Example

```
cluster1::*> network interface show -allow-lb-migrate true
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0	data1	up/up	192.0.2.120/24	node0	e0e	true
	data2	up/up	192.0.2.121/24	node0	e0f	true
	data3	up/up	192.0.2.122/24	node1	e0e	true
	data4	up/up	192.0.2.123/24	node1	e0f	true
	data5	up/up	192.0.2.124/24	node2	e0e	true
	data6	up/up	192.0.2.125/24	node2	e0f	true
	data7	up/up	192.0.2.126/24	node3	e0e	true
	data8	up/up	192.0.2.127/24	node3	e0f	true

8 entries were displayed.

You should record which LIFs have automatic rebalancing enabled so that you can reenable it after the batch upgrade is completed.

3. Disable automatic LIF rebalancing for each LIF that you identified:

```
network interface modify * -allow-lb-migrate false
```

4. Return to the admin privilege level:

```
set -privilege admin
```

Identifying active CIFS sessions that should be terminated

Before performing a minor nondisruptive upgrade or downgrade within the Data ONTAP 8.2 release family, you should identify and gracefully terminate any CIFS sessions that are not continuously available.

About this task

Continuously available CIFS shares, which are accessed by Hyper-V clients using the SMB3 protocol, do not need to be terminated before upgrading or downgrading.

Steps

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.

Example

```
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: CIFS\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.

```

Each of the sessions identified by this command should be terminated before proceeding with the Data ONTAP upgrade or downgrade.

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
```

Example

```

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 concepts

Considerations for session-oriented protocols on page 168

Verifying the system time

You should verify that NTP is configured, and that the time is synchronized across the cluster.

About this task

For more information about managing the system time, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

1. Use the system services `ntp server show` command to verify that each node is associated with an NTP server.

Example

```
cluster1::> system services ntp server show
Node  Server                      Version
-----
node0  ntp1.example.com             max
       ntp2.example.com             max
node1  ntp1.example.com             max
       ntp2.example.com             max
node2  ntp1.example.com             max
       ntp2.example.com             max
node3  ntp1.example.com             max
       ntp2.example.com             max
```

2. Verify that each node has the same date and time:

If you are running Data ONTAP...	Enter the following command...
8.1.x	<code>system node date show</code>
8.2.x	<code>cluster date show</code>

Example

```
cluster1::> cluster date show
Node  Date                        Timezone
-----
node0  4/6/2013 20:54:38          GMT
node1  4/6/2013 20:54:38          GMT
node2  4/6/2013 20:54:38          GMT
node3  4/6/2013 20:54:38          GMT
4 entries were displayed.
```


Determining the current software version on each node

For a successful upgrade, each node must be running the minimum software version allowed for the upgrade. You can check the software version by running the `system node image show` command.

About this task

Only clusters running Data ONTAP 8.1 or later can be upgraded directly to Data ONTAP 8.2.x.

Step

1. Determine the current software version:

`system node image show`

Example

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

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	8.1.2	10/25/2012 12:36:46
	image2	false	false	8.1.0	11/27/2011 12:58:24
node1	image1	true	true	8.1.2	10/25/2012 12:34:22
	image2	false	false	8.1.0	11/27/2011 12:58:26

4 entries were displayed.

Obtaining Data ONTAP software images

You must copy a software image from the NetApp Support Site to an HTTP or FTP server on your network so that nodes can access the images by using the `system node image update` command.

About this task

To upgrade, revert, or downgrade the cluster to the target release of Data ONTAP, you need access to software images. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site. Note the following important information:

- Software images are specific to platform models.
Be sure to obtain the correct image for your cluster.
- Software images include the latest version of system firmware that was available when a given version of Data ONTAP was released.

Steps

1. Locate the target Data ONTAP software in the **Software Downloads** area of the NetApp Support Site.

2. Copy the software image (for example, `821_q_image.tgz`) from the NetApp Support Site to the directory on the HTTP or FTP server from which the image will be served.

Related information

[Download Software: support.netapp.com/NOW/cgi-bin/software](http://support.netapp.com/NOW/cgi-bin/software)

Installing Data ONTAP software images in a cluster

If needed, install the target Data ONTAP 8.x image software package, but leave the default set to the current Data ONTAP 8.x version.

Before you begin

You must have obtained the Data ONTAP software images.

Steps

1. Choose one of the following options based on your requirements:

If you want to...	Enter this command...
Download, but not install, the software image	<pre>system node image get -node * -package location -replace-package true -background true</pre> <p>This command downloads the software image to all of the nodes simultaneously. To download the image to each node one at a time, do not specify the <code>-background</code> parameter.</p>
Install a previously downloaded software image	<pre>system node image update -node * -package file:///mroot/etc/software/image_name -background true</pre> <p>Note the following considerations for this command:</p> <ul style="list-style-type: none">• If you are currently running Data ONTAP 8.2, the <code>-package</code> parameter only requires you to enter the image name; you do not need to enter the full directory path.• If you are unsure of the image name to install, you can view a list of previously downloaded software images by using the <code>system node image package show</code> command.• This command installs the software image on all of the nodes simultaneously. To install the image on each node one at a time, do not specify the <code>-background</code> parameter.
Download and install the software image in the same operation	<pre>system node image update -node * -package location -replace-package true -background true</pre> <p>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 <code>-background</code> parameter.</p>

2. 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`.

Example

This example shows a 2-node cluster in which the software image has been 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:    Installation complete. image2 updated on node node0.
There is no update/install in progress
Status of most recent operation:
  Run Status:      Exited
  Exit Status:     Success
  Phase:           Run Script
  Exit Message:    Installation complete. image2 updated on node node1.
2 entries were acted on.
```

How Data ONTAP software images are stored and alternated in the cluster

Each node in the cluster can hold two Data ONTAP software images, the current image that is running, and an alternate image that you can boot.

You can view the software images on each node in the cluster by using the `system node image show` command. The following example shows how the images alternate when you download a new software image and then upgrade to it.

How Data ONTAP images alternate

This example shows a two-node cluster. Each node has two images, *image1* (version 8.0.2) and *image2* (version 8.0.1). Both nodes are currently running *image1*, as indicated by the `Is Current` column. If you were to reboot either node, it would boot *image1*, because that is the default image (indicated by the `Is Default` column). The alternate image on both nodes is *image2*.

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

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	8.0.2	3/25/2011 12:36:46
	image2	false	false	8.0.1	10/15/2010 12:58:24
node1					

```

image1 true true 8.0.2 3/25/2011 12:34:22
image2 false false 8.0.1 10/15/2010 12:58:26
4 entries were displayed.

```

If you were to download a new software image, the new package would replace the package in the alternate image (*image2*) while all of the nodes continue to run the current image (*image1*).

```

cluster1::> system node image update -node * -package http://
10.28.99.99/8.1.1_q_image.tgz -replace-package true

```

After the download completes, the 8.1.1 version is now stored as the alternate image (*image2*), while both nodes continue to run version 8.0.2 (*image1*).

```

cluster1::> system node image show

```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	8.0.2	3/25/2011 12:36:46
	image2	false	false	8.1.1	6/15/2012 10:23:18
node1	image1	true	true	8.0.2	3/25/2011 12:34:22
	image2	false	false	8.1.1	6/15/2012 10:23:18

```

4 entries were displayed.

```

If you use the `system node image modify` command to set *image2* as the default image on the nodes, then after you reboot a node, it will boot *image2*. In this example, *image2* has been set to the default image, and the nodes have been rebooted. The images have alternated: *image1* is now the alternate image, and *image2* is the current image.

```

cluster1::> system node image show

```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	false	false	8.0.2	3/25/2011 12:36:46
	image2	true	true	8.1.1	6/15/2012 10:23:18
node1	image1	false	false	8.0.2	3/25/2011 12:34:22
	image2	true	true	8.1.1	6/15/2012 10:23:18

```

4 entries were displayed.

```

Preparing SnapMirror relationships for a nondisruptive upgrade or downgrade

You must suspend SnapMirror operations before performing a nondisruptive upgrade or downgrade of Data ONTAP.

About this task

For more information about SnapMirror operations, see the SnapMirror man pages and the *Clustered Data ONTAP Data Protection Guide*.

Steps

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`.

Example

If you are upgrading from Data ONTAP 8.1, this example quiesces transfers involving the destination volume `vol1` from Storage Virtual Machine (SVM) `vs0` and cluster `cluster1`:

```
cluster1::> snapmirror quiesce -destination-path cluster1://vs0/vol1
```

Example

If you are downgrading within the Data ONTAP 8.2 release family, this example quiesces transfers involving the destination volume `vol1` from SVM `vs0`:

```
cluster1::> snapmirror quiesce -destination-path vs0:vol1
```

3. Verify that all SnapMirror relationships are quiesced:

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

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

Example

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 transferring, do one of the following options:

Option	Description
Wait for the transfers to complete before performing the Data ONTAP upgrade.	Once each transfer completes, the relationship changes to <i>Quiesced</i> status.
Stop the transfers by entering the following command: snapmirror abort -destination-path destination -h 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 <i>Quiesced</i> status.

Ensuring that no jobs are running

You must verify the status of cluster jobs before upgrading or downgrading to a different Data ONTAP release. 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, allow the jobs to finish successfully or stop the queued entries.

Steps

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

```
job show
```

Example

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

Job ID	Name	Owning Vserver	Node	State
8629	Vol Reaper	cluster1	-	Queued
8630	Description: Vol Reaper Job			
	Certificate Expiry Check	cluster1	-	Queued
	Description: Certificate Expiry Check			
8632	CLUSTER BACKUP AUTO daily	cluster1	-	Queued
	Description: Cluster Backup Job			
8633	CLUSTER BACKUP AUTO weekly	cluster1	-	Queued
	Description: Cluster Backup Job			
9944	SnapMirrorDaemon_7_2147484678	cluster1	node1	Dormant
	Description: Snapmirror Daemon for 7_2147484678			
18277	CLUSTER BACKUP AUTO 8hour	cluster1	-	Queued
	Description: Cluster Backup Job			
18377	SnapMirror Service Job	cluster1	node0	Dormant
	Description: SnapMirror Service Job			

```

18379 Network Consistency Diagnostic - weekly
      cluster1 node0 Queued
      Description: Network Consistency Checker
18385 Network Consistency Diagnostic - weekly
      cluster1 node1 Queued
      Description: Network Consistency Checker
9 entries were displayed

```

2. Delete any running or queued aggregate, volume, or Snapshot copy jobs:

```
job delete -id job_id
```

Example

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

3. Ensure that no aggregate, volume, or Snapshot jobs are running or queued:

```
job show
```

Example

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

```

Performing the software upgrade

To upgrade a cluster to a new Data ONTAP release, you must verify that the cluster is ready to be upgraded, choose an upgrade method, and then perform the steps for the upgrade method.

You can select one of the following upgrade methods:

- Rolling upgrade (nondisruptive)
- Batch upgrade (nondisruptive)
- Disruptive upgrade

Related concepts

[Types of cluster upgrades](#) on page 11

Verifying that the cluster is ready to be upgraded

You must verify that the target Data ONTAP software is installed, storage failover is enabled, and if necessary, cluster HA is enabled.

Steps

1. Verify that the Data ONTAP 8.2 software is installed:

```
system node image show
```

Example

This example shows that version 8.2.1 is installed as the alternate image on both nodes.

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

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	8.1.2	10/25/2012 12:37:36
	image2	false	false	8.2.1	11/22/2013 13:52:22
node1	image1	true	true	8.1.2	10/25/2012 12:41:16
	image2	false	false	8.2.1	11/22/2013 13:55:22

4 entries were displayed.

For more information about installing the target Data ONTAP software image, see [Installing Data ONTAP 8.x software images in a cluster](#).

2. Set the Data ONTAP 8.2 software image to be the default image:

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

3. Verify that the Data ONTAP 8.2 software image is set as the default image:

```
system node image show
```

Example

This example shows that version 8.2.1 is set as the default image on both nodes.

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

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	false	true	8.1.2	10/25/2012 12:37:36
	image2	true	false	8.2.1	11/22/2013 13:52:22
node1	image1	false	true	8.1.2	10/25/2012 12:41:16
	image2	true	false	8.2.1	11/22/2013 13:55:22

4 entries were displayed.

4. If you are performing a nondisruptive upgrade, verify the high availability configuration:
 - a. Verify that storage failover is enabled and possible:


```
storage failover show
```

Example

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.
```

You can enable storage failover by using the `storage failover modify` command.

- b. If the cluster consists of only two nodes (a single HA pair), ensure that cluster HA is configured:

```
cluster ha show
```

Example

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

You can enable cluster HA by using the `cluster ha modify` command.

Upgrading a Data ONTAP cluster nondisruptively by using the rolling upgrade method

This nondisruptive upgrade (NDU) 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.

Before you begin

You must have satisfied upgrade preparation requirements and verified that the cluster is ready to be upgraded.

Steps

1. If this is a four-node cluster, use the `cluster show` command at the advanced privilege level to determine which node holds epsilon.

In a four-node cluster, the node that holds epsilon should always be online to ensure that the cluster can remain in quorum and continue serving data even if a node unexpectedly goes out of service during the upgrade. Therefore, if the cluster is a four-node cluster, the node that holds epsilon should be upgraded last. After the first three nodes have been upgraded, you can transfer epsilon to a node in the first HA pair and then upgrade the last node.

If you are upgrading a cluster of any other size, you do not need to consider epsilon during the upgrade. Two-node clusters do not use epsilon, and clusters with more than four nodes remain in quorum even if a node unexpectedly goes out of service while the node holding epsilon is being upgraded.

2. [Upgrading the first node in an HA pair](#) on page 50

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.

3. [Upgrading the second node in an HA pair](#) on page 55

After upgrading 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.

4. [Verifying that the HA pair was upgraded successfully](#) on page 60

After upgrading both nodes in an HA pair, you must verify that the target release is running on both nodes.

5. Repeat Steps 2-4 for each additional HA pair.

After you finish

You should complete post-upgrade tasks.

Related references

[Cluster upgrade checklist](#) on page 11

Upgrading 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.

Steps

1. Disable automatic giveback on both nodes of the HA pair if it is enabled by entering the following command on each node:

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

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

2. Verify that automatic giveback is disabled for both nodes:

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

Example

```
cluster1:>> storage failover show -fields auto-giveback
node      auto-giveback
```

```

-----
node0      false
node1      false
2 entries were displayed.

```

3. Determine whether the node to be upgraded is currently serving any clients by entering the following command twice:

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

The `uptime` command displays the total number of operations the node has performed for NFS, CIFS, FC, and iSCSI clients since the node was last booted. For each protocol, determine if the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

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

Example

This 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

```

4. Migrate LIFs away from the node:

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

Data LIFs for SAN protocols are not migrated. As long as these LIFs exist on each node in the cluster, data can be served through alternate paths during the upgrade process.

If you are connected to the cluster through the cluster management LIF, and if this node currently hosts the cluster management LIF, then your SSH session will be temporarily disconnected while the LIF is migrated. After the LIF has migrated, you can log in to the cluster through the cluster management LIF.

5. Use the `network interface show` command to verify that the LIFs migrated away from the node.

Example

This 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      e0c      node1     e0c      up          up

```

```
vs0      data002 node0      e0d      node1      e0d      up      up
vs0      data003 node0      e0d      node1      e0d      up      up
vs0      data004 node0      e0c      node1      e0c      up      up
4 entries were displayed.
```

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

6. Trigger an AutoSupport notification:

```
system node autosupport invoke -node nodenameA -type all -message "starting_NDU"
```

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

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

7. Initiate a takeover:

```
storage failover takeover -ofnode nodenameA
```

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

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 safely ignore this notification and proceed with the upgrade.

8. Verify that the takeover was successful:

```
storage failover show
```

Example

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

```
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.
```

9. Wait 8 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 may take longer than 8 minutes depending on the characteristics of the client applications.

10. Return the aggregates to the first node:

```
storage failover giveback -ofnode nodenameA
```

Attention: The giveback is not initiated, an error message is returned, and an event is generated if any conditions such as the following are detected:

- Long-running operations (such as ASUP generation)
- Operations that cannot be restarted (such as aggregate creation)
- Error conditions (such as a disk connectivity mismatch between the nodes)

If giveback is not initiated, complete the following steps:

- a. Address the "veto" condition described in the error message, ensuring that any identified operations are terminated gracefully.

- b. Reenter the giveback command:

```
storage failover giveback -ofnode nodenameA
```

Alternatively, you can analyze the messages and events for relevance in your environment. If you determine that the veto conditions are not significant, you can override the giveback veto by entering the following command:

```
storage failover giveback -ofnode nodenameA -override-vetoes true
```

For more information about determining whether you can safely override the veto, see the *Clustered Data ONTAP High-Availability Configuration Guide*.

This first returns the root aggregate to the partner node and then, after that node has finished booting, returns the non-root aggregates.

11. Verify that all aggregates have been returned:

```
storage failover show-giveback
```

If the Giveback Status field indicates that the node that was taken over is in partial giveback, then complete the following steps before proceeding:

- a. Determine which aggregates have been returned:

```
storage aggregate show -node nodenameA
```

- b. Check EMS logs for errors and take corrective action.

For more information about EMS messages, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

- c. Repeat Step 11.a on page 53 to verify any corrections.

The newly-booted node begins to serve data to clients from each aggregate as soon as the aggregate is returned.

12. Wait 8 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 may take longer than 8 minutes depending on the characteristics of the client applications.

13. Verify that the upgrade completed successfully for the node:

- a. Set the privilege level to advanced:

```
set -privilege advanced
```

- b. Ensure that upgrade 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 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.

- c. Return to the admin privilege level:

```
set -privilege admin
```

14. Revert the LIFs back to the node:

```
network interface revert *
```

Example

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

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

15. Verify that the node's data ports and LIFs are up and operational:

- a. Verify that the node's data ports are up:

```
network port show -node nodenameA -role data
```

Example

This example shows that all of the node's data ports are up.

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

Node	Port	Role	Link	MTU	Auto-Negot Admin/Oper	Duplex Admin/Oper	Speed (Mbps) Admin/Oper
node0	e0c	data	up	9000	true/true	full/full	auto/1000
	e0d	data	up	9000	true/true	full/full	auto/1000
	e1b	data	up	9000	true/true	full/full	auto/1000
	e1c	data	up	9000	true/true	full/half	auto/10
	e1d	data	up	9000	true/true	full/half	auto/10

5 entries were displayed.

- b. Verify that the node's data LIFs successfully reverted back to the node, and that they are up:

```
network interface show -data-protocol nfs|cifs -role data -curr-node  
nodenameA
```

Example

This example shows that all of the data LIFs hosted by the node have successfully reverted back to the node, and that they are operationally up.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data -curr-node node0
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          e0c      true
      data002      up/up      192.0.2.121/24      node0          e0d      true
      data003      up/up      192.0.2.122/24      node0          e0d      true
      data004      up/up      192.0.2.123/24      node0          e0c      true
4 entries were displayed.
```

16. 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 upgrade.

Example

This example shows that the upgraded 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
```

17. Trigger an AutoSupport notification:

```
system node autosupport invoke -node nodenameA -type all -message "finishing_NDU"
```

Upgrading the partner node in an HA pair

After upgrading 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.

Steps

1. If you are upgrading a four-node cluster, and if this is the last node to be upgraded, then transfer epsilon to a node in the first HA pair.

Transferring epsilon to a node in the first HA pair helps to prevent the cluster from falling out of quorum if another node unexpectedly goes out of service while the last node is being upgraded.

- a. Set the privilege level to advanced:

```
set -privilege advanced
```

- b. Mark epsilon false on the node:

```
cluster modify -node nodename -epsilon false
```

- c. Mark epsilon true on the first node that was upgraded:

```
cluster modify -node nodename -epsilon true
```

- d. Return to the admin privilege level:

```
set -privilege admin
```

- Determine whether the node to be upgraded is currently serving any clients by entering the following command twice:

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

The `uptime` command displays the total number of operations the node has performed for NFS, CIFS, FC, and iSCSI clients since the node was last booted. For each protocol, determine if the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

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

Example

This 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
```

- Migrate LIFs away from the node:

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

Data LIFs for SAN protocols are not migrated. As long as these LIFs exist on each node in the cluster, data can be served through alternate paths during the upgrade process.

If you are connected to the cluster through the cluster management LIF, and if this node currently hosts the cluster management LIF, then your SSH session will be temporarily disconnected while the LIF is migrated. After the LIF has migrated, you can log in to the cluster through the cluster management LIF.

- Use the `network interface show` command to verify that the LIFs migrated away from the node.

Example

This 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
vs0      lif      home-node home-port curr-node curr-port status-oper status-admin
-----
vs0      data005 node1     e0c      node0     e0c      up         up
vs0      data006 node1     e0d      node0     e0d      up         up
vs0      data007 node1     e0d      node0     e0d      up         up
vs0      data008 node1     e0c      node0     e0c      up         up
4 entries were displayed.
```


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

5. Trigger an AutoSupport notification:

```
system node autosupport invoke -node nodenameB -type all -message "starting_NDU"
```

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

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

6. Initiate a takeover by using one of the following commands:

If you are upgrading from a... Enter this command...

Data ONTAP 8.2.x release	storage failover takeover -ofnode nodenameB
--------------------------	--

Data ONTAP 8.1.x release	storage failover takeover -ofnode nodenameB -option allow-version-mismatch
--------------------------	---

The `allow-version-mismatch` option enables the HA pair to tolerate different Data ONTAP release family versions during a major release upgrade.

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

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 safely ignore this notification and proceed with the upgrade.

7. Verify that the takeover was successful:

```
storage failover show
```

Example

This example shows that the takeover was successful. Node `node1` is in the `Waiting for giveback` state, and its partner is `In takeover`.

```
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.
```

8. Wait 8 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 may take longer than 8 minutes depending on the characteristics of the client applications.

9. Return the aggregates to the partner node:

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

Attention: The giveback is not initiated, an error message is returned, and an event is generated if any conditions such as the following are detected:

- Long-running operations (such as ASUP generation)
- Operations that cannot be restarted (such as aggregate creation)
- Error conditions (such as a disk connectivity mismatch between the nodes)

If giveback is not initiated, complete the following steps:

- Address the "veto" condition described in the error message, ensuring that any identified operations are terminated gracefully.
- Reenter the giveback command:

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

Alternatively, you can analyze the messages and events for relevance in your environment. If you determine that the veto conditions are not significant, you can override the giveback veto by entering the following command:

```
storage failover giveback -ofnode nodenameB -override-vetoes true
```

For more information about determining whether you can safely override the veto, see the *Clustered Data ONTAP High-Availability Configuration Guide*.

This first returns the root aggregate to the partner node and then, after that node has finished booting, returns the non-root aggregates.

10. Verify that all aggregates have been returned:

```
storage failover show-giveback
```

If the `Giveback Status` field indicates that the node that was taken over is in partial giveback, then complete the following steps before proceeding:

- Determine which aggregates have been returned:

```
storage aggregate show -node nodenameB
```
- Check EMS logs for errors and take corrective action.

For more information about EMS messages, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

- Repeat Step [10.a](#) on page 58 to verify any corrections.

The newly-booted node begins to serve data to clients from each aggregate as soon as the aggregate is returned.

11. Wait 8 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 may take longer than 8 minutes depending on the characteristics of the client applications.

12. Verify that the upgrade completed successfully for the node:

- a. Set the privilege level to advanced:

```
set -privilege advanced
```

- b. Ensure that upgrade 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 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.

- c. Return to the admin privilege level:

```
set -privilege admin
```

13. Revert the LIFs back to the node:

```
network interface revert *
```

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

Example

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

14. Verify that the node's data ports and LIFs are up and operational:

- a. Verify that the node's data ports are up:

```
network port show -node nodenameB -role data
```

Example

This example shows that all of the node's data ports are up.

```
cluster1::> network port show -node node1 -role data
Node  Port  Role  Link  MTU  Auto-Negot  Duplex  Speed (Mbps)
-----
node1
      e0c   data  up    9000  true/true  full/full  auto/1000
      e0d   data  up    9000  true/true  full/full  auto/1000
      e1b   data  up    9000  true/true  full/full  auto/1000
      e1c   data  up    9000  true/true  full/half  auto/10
      e1d   data  up    9000  true/true  full/half  auto/10
5 entries were displayed.
```

- b. Verify that the node's data LIFs successfully reverted back to the node, and that they are up:

```
network interface show -data-protocol nfs|cifs -role data -curr-node  
nodenameB
```

Example

This example shows that all of the data LIFs hosted by the node have successfully reverted back to the node, and that they are operationally up.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data -curr-node node1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0	data001	up/up	192.0.2.120/24	node1	e0c	true
	data002	up/up	192.0.2.121/24	node1	e0d	true
	data003	up/up	192.0.2.122/24	node1	e0d	true
	data004	up/up	192.0.2.123/24	node1	e0c	true

4 entries were displayed.

15. 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 upgrade.

Example

This example shows that the upgraded 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

16. Trigger an AutoSupport notification:

```
system node autosupport invoke -node nodenameB -type all -message  
"finishing_NDU"
```

Verifying that the HA pair was upgraded successfully

After upgrading both nodes in an HA pair, you must verify that the target release is running on both nodes.

Steps

1. Confirm that the new Data ONTAP 8.2.x software is running on both nodes of the HA pair:

```
system node image show
```

Example

This example shows version 8.2.1 as the current version on both nodes:

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

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	8.2.1	11/22/2013 13:52:22
	image2	false	false	8.1.2	10/25/2012 12:37:36
node1	image1	true	true	8.2.1	11/22/2013 13:55:22
	image2	false	false	8.1.2	10/25/2012 12:41:16

4 entries were displayed.

2. Re-enable automatic giveback on both nodes if it was previously disabled:

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

3. Ensure that the cluster is in quorum and that services are running before upgrading the next pair of nodes.

You can use the `cluster show` and `cluster ring show` commands to verify that the cluster is in quorum.

After you finish

Upgrade any additional HA pairs. After all of the HA pairs are upgraded, you should verify that the cluster was upgraded successfully.

Upgrading a Data ONTAP cluster nondisruptively by using the batch method

If your cluster contains eight or more nodes, you can upgrade Data ONTAP by dividing the cluster into two upgrade batches, upgrading a set of nodes in the first batch, upgrading their high-availability partners, and then repeating the process for the second batch.

Before you begin

- You must have completed the upgrade preparation requirements and verified that the cluster is ready to be upgraded.
- You must have determined the upgrade sequence for the batch upgrade.

About this task

If the cluster serves SAN clients, do not use the batch upgrade method. You should perform a rolling upgrade instead.

Steps

1. [Upgrading the first set of nodes in a batch of HA pairs](#) on page 62

You upgrade the first set of nodes in a batch of HA pairs by initiating a takeover by the nodes' partners. The partners serve the nodes' data while the first set of nodes is upgraded.

2. [Upgrading the second set of nodes in a batch of HA pairs](#) on page 68

You upgrade the partner nodes in a batch of HA pairs by initiating a takeover on the nodes. The first set of nodes serve the nodes' data while the partners are upgraded.

3. *Verifying that the batch was upgraded successfully* on page 73

After upgrading all of the nodes in a batch, you must verify that the target release is running on the nodes.

4. Repeat Steps 1-3 to upgrade the second batch.

After you finish

You should verify that the cluster was upgraded successfully.

Related concepts

Required upgrade sequence for a batch upgrade on page 19

Related references

Cluster upgrade checklist on page 11

Upgrading the first set of nodes in a batch of HA pairs

You upgrade the first set of nodes in a batch of HA pairs by initiating a takeover by the nodes' partners. The partners serve the nodes' data while the first set of nodes is upgraded.

Steps

1. Disable automatic giveback on the HA pairs in the first batch by entering the following command on each node:

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

2. Verify that automatic giveback is disabled for the nodes in the batch:

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

Example

This example shows that automatic giveback has been disabled on all of the nodes in the batch.

```
cluster1:> storage failover show -fields auto-giveback
node      auto-giveback
-----
node0     false
node1     false
node2     false
node3     false
node4     false
node5     false
node6     true
node7     true
node8     true
node9     true
node10    true
```

```
node11    true
12 entries were displayed.
```

3. 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 nodename -command uptime
```

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

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

Example

This 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
```

4. Migrate LIFs away from the nodes that will be taken over by entering the following command for each node in the first set:

```
network interface migrate {-data-protocol nfs|cifs -role data -curr-node source_node} -dest-node partner_node
```

This command migrates the node's data LIFs to its high-availability partner, which will take over the node's storage while the node is upgraded. If the partner cannot host the node's data LIFs, such as if the partner does not have a port on the same subnet, you can migrate the LIFs to any other node that will remain up while the first node is upgraded.

Data LIFs for SAN protocols are not migrated. As long as these LIFs exist on each node in the cluster, data can be served through alternate paths during the upgrade process.

5. Verify that the LIFs migrated to the proper ports on the nodes' partners by entering the following command for each node's partner:

```
network interface show -data-protocol nfs|cifs -role data -curr-node partner_node
```

Example

This example shows that node0's data LIFs were migrated to port e0b on its partner (node1).

```
cluster1:> network interface show -data-protocol nfs|cifs -role data -curr-node node1
Logical      Status      Network      Current      Current Is
```

Vserver	Interface	Admin/Oper	Address/Mask	Node	Port	Home
vs0						
	lif1	up/up	192.0.2.130/24	node1	e0b	true
	lif2	up/up	192.0.2.131/24	node1	e0b	false
	lif3	up/up	192.0.2.132/24	node1	e0b	true
vs1						
	lif1	up/up	192.0.2.133/24	node1	e0b	false
	lif2	up/up	192.0.2.134/24	node1	e0b	true
5 entries were displayed.						

If desired, you can migrate a LIF to a different port on the partner node by using the `network interface migrate` command.

6. Trigger an AutoSupport notification by entering the following command for each node in the set:

```
system node autosupport invoke -node nodename -type all -message "starting_NDU"
```

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

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

7. Initiate a takeover by entering the following command for each node in the first set:

```
storage failover takeover -ofnode nodename
```

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

The nodes boot up to the `Waiting for giveback` state.

Note: 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.

8. Verify that the takeover was successful:

```
storage failover show
```

Example

This example shows that the takeover was successful. The first set of nodes (node0, node2, and node4) are in the `Waiting for giveback` state, and their partners are `In takeover`.

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

Node	Partner	Takeover Possible	State Description
node0	node1	-	Waiting for giveback (HA mailboxes)
node1	node0	false	In takeover
node2	node3	-	Waiting for giveback (HA mailboxes)
node3	node2	false	In takeover
node4	node5	-	Waiting for giveback (HA mailboxes)
node5	node4	false	In takeover
node6	node7	true	Connected to node7
node7	node6	true	Connected to node6
node8	node9	true	Connected to node9
node9	node8	true	Connected to node8
node10	node11	true	Connected to node11


```
node11      node10      true      Connected to node10
12 entries were displayed.
```

9. Wait 8 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 may take longer than 8 minutes depending on the characteristics of the client applications.

10. Return the aggregates to the nodes by entering the following command for each of the nodes' partners:

```
storage failover giveback -ofnode nodename
```

Attention: The giveback is not initiated, an error message is returned, and an event is generated if any conditions such as the following are detected:

- Long-running operations (such as ASUP generation)
- Operations that cannot be restarted (such as aggregate creation)
- Error conditions (such as a disk connectivity mismatch between the nodes)

If giveback is not initiated, complete the following steps:

- a. Address the "veto" condition described in the error message, ensuring that any identified operations are terminated gracefully.
- b. Reenter the giveback command:

```
storage failover giveback -ofnode nodename
```

Alternatively, you can analyze the messages and events for relevance in your environment. If you determine that the veto conditions are not significant, you can override the giveback veto by entering the following command:

```
storage failover giveback -ofnode nodename -override-vetoes true
```

For more information about determining whether you can safely override the veto, see the *Clustered Data ONTAP High-Availability Configuration Guide*.

This first returns the root aggregate to the partner nodes and then, after those nodes have finished booting, returns the non-root aggregates.

11. Verify that all aggregates have been returned:

```
storage failover show-giveback
```

If the Giveback Status field indicates that a node that was taken over is in partial giveback, then complete the following steps before proceeding:

- a. Determine which aggregates have been returned:

```
storage aggregate show -node nodename
```

- b. Check EMS logs for errors and take corrective action.

For more information about EMS messages, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

- c. Repeat Step 11.a on page 65 to verify any corrections.

The newly-booted nodes begin to serve data to clients from each aggregate as soon as the aggregate is returned.

12. Wait 8 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 may take longer than 8 minutes depending on the characteristics of the client applications.

13. Verify that the upgrade completed successfully for the nodes in the first set:

- a. Set the privilege level to advanced:

```
set -privilege advanced
```

- b. Ensure that upgrade status is complete for each node in the first set:

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

The status should be listed as complete.

If the status is not successful for any node in the set, 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.

- c. Return to the admin privilege level:

```
set -privilege admin
```

14. Revert the LIFs back to the first set of nodes:

```
network interface revert *
```

Example

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

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

15. Verify that the nodes' data ports and LIFs are up and operational by completing the following steps for each node in the first set:

- a. Verify that the data ports are up for each node in the first set:

```
network port show -node nodename -role data
```

Example

This example shows that all of a node's data ports are up.

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

Node	Port	Role	Link	MTU	Auto-Negot Admin/Oper	Duplex Admin/Oper	Speed (Mbps) Admin/Oper
node0	e0c	data	up	9000	true/true	full/full	auto/1000
	e0d	data	up	9000	true/true	full/full	auto/1000
	e1b	data	up	9000	true/true	full/full	auto/1000
	e1c	data	up	9000	true/true	full/half	auto/10
	e1d	data	up	9000	true/true	full/half	auto/10

5 entries were displayed.

- b. Verify that data LIFs successfully reverted back to each node in the first set, and that the LIFs are up:

```
network interface show -data-protocol nfs|cifs -role data -curr-node nodename
```

Example

This example shows that all of the data LIFs hosted by a node have successfully reverted back to the node, and that they are up.

```
cluster1:> network interface show -data-protocol nfs|cifs -role data -curr-node node0
```

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	e0c	true
	data002	up/up	192.0.2.121/24	node0	e0d	true
	data003	up/up	192.0.2.122/24	node0	e0d	true
	data004	up/up	192.0.2.123/24	node0	e0c	true

4 entries were displayed.

16. If you previously determined that any of the nodes in the first set serve clients, verify that each node is providing service for each protocol that it was previously serving:

```
system node run -node nodename -command uptime
```

The operation counts reset to zero during the upgrade.

Example

This example shows that an upgraded 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

17. Trigger an AutoSupport notification by entering the following command for each of the nodes in the first set:

```
system node autosupport invoke -node nodename -type all -message "finishing_NDU"
```

Upgrading the partner nodes in a batch of HA pairs

You upgrade the partner nodes in a batch of HA pairs by initiating a takeover on the nodes. The first set of nodes serve the nodes' data while the partners are upgraded.

Steps

1. 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 nodename -command uptime
```

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

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

Example

This 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
```

2. Migrate LIFs away from the nodes that will be taken over by entering the following command for each node in the second set:

```
network interface migrate {-data-protocol nfs|cifs -role data -curr-node  
source_node} -dest-node partner_node
```

This command migrates the node's data LIFs to its high-availability partner, which will take over the node's storage while the node is upgraded. If the partner cannot host the node's data LIFs, such as if the partner does not have a port on the same subnet, you can migrate the LIFs to any other node that will remain up while the first node is upgraded.

Data LIFs for SAN protocols are not migrated. As long as these LIFs exist on each node in the cluster, data can be served through alternate paths during the upgrade process.

3. Verify that the LIFs migrated to the proper ports on the nodes' partners by entering the following command for each node's partner:

```
network interface show -data-protocol nfs|cifs -role data -curr-node  
partner_node
```

Example

This example shows that node1's data LIFs were migrated to port e0b on its partner (node0).

```
cluster1::> network interface show -data-protocol nfs|cifs -role data -curr-node node0
Logical      Status      Network      Current      data      -curr-node node0
Vserver      Interface  Admin/Oper   Address/Mask Node          Current Is
-----
vs0
    lif1      up/up      192.0.2.130/24 node0        e0b      false
    lif2      up/up      192.0.2.131/24 node0        e0b      true
    lif3      up/up      192.0.2.132/24 node0        e0b      false
vs1
    lif1      up/up      192.0.2.133/24 node0        e0b      true
    lif2      up/up      192.0.2.134/24 node0        e0b      false
5 entries were displayed.
```

If desired, you can migrate a LIF to a different port on the partner node by using the `network interface migrate` command.

4. Trigger an AutoSupport notification by entering the following command for each of the nodes in the second set:

```
system node autosupport invoke -node nodename -type all -message "starting_NDU"
```

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

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

5. Initiate a takeover by entering one of the following commands for each node in the second set:

If you are upgrading from a... Enter this command...	
Data ONTAP 8.2.x release	storage failover takeover -ofnode nodename
Data ONTAP 8.1.x release	storage failover takeover -ofnode nodename -option allow-version-mismatch
	The <code>allow-version-mismatch</code> option enables the HA pair to tolerate different Data ONTAP release family versions during a major release upgrade.

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

The nodes that are taken over boot up to the `Waiting for giveback` state.

Note: 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.

6. Verify that the takeover was successful:

```
storage failover show
```

Example

This example shows that the takeover was successful. The second set of nodes (node1, node3, and node5) are in the Waiting for giveback state, and their partners are In takeover.

```
cluster1::> storage failover show
Node           Partner      Takeover
Possible State Description
-----
node0          node1         false    In takeover
node1          node0         -        Waiting for giveback (HA mailboxes)
node2          node3         false    In takeover
node3          node2         -        Waiting for giveback (HA mailboxes)
node4          node5         false    In takeover
node5          node4         -        Waiting for giveback (HA mailboxes)
node6          node7         true     Connected to node7
node7          node6         true     Connected to node6
node8          node9         true     Connected to node9
node9          node8         true     Connected to node8
node10         node11        true     Connected to node11
node11         node10        true     Connected to node10
12 entries were displayed.
```

7. Wait 8 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 may take longer than 8 minutes depending on the characteristics of the client applications.

8. Return the aggregates to the nodes by entering the following command for each of the nodes' partners:

```
storage failover giveback -ofnode nodename
```

Attention: The giveback is not initiated, an error message is returned, and an event is generated if any conditions such as the following are detected:

- Long-running operations (such as ASUP generation)
- Operations that cannot be restarted (such as aggregate creation)
- Error conditions (such as a disk connectivity mismatch between the nodes)

If giveback is not initiated, complete the following steps:

- Address the "veto" condition described in the error message, ensuring that any identified operations are terminated gracefully.
- Reenter the giveback command:

```
storage failover giveback -ofnode nodename
```

Alternatively, you can analyze the messages and events for relevance in your environment. If you determine that the veto conditions are not significant, you can override the giveback veto by entering the following command:

```
storage failover giveback -ofnode nodename -override-vetoes true
```

For more information about determining whether you can safely override the veto, see the *Clustered Data ONTAP High-Availability Configuration Guide*.

This first returns the root aggregate to the partner nodes and then, after those nodes have finished booting, returns the non-root aggregates.

9. Verify that all aggregates have been returned:

storage failover show-giveback

If the `Giveback Status` field indicates that a node that was taken over is in partial giveback, then complete the following steps before proceeding:

- a. Determine which aggregates have been returned:

storage aggregate show -node nodename

- b. Check EMS logs for errors and take corrective action.

For more information about EMS messages, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

- c. Repeat Step 9.a on page 71 to verify any corrections.

The newly-booted nodes begin to serve data to clients from each aggregate as soon as the aggregate is returned.

10. Wait 8 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 may take longer than 8 minutes depending on the characteristics of the client applications.

11. Verify that the upgrade completed successfully for the nodes in the second set:

- a. Set the privilege level to advanced:

set -privilege advanced

- b. Ensure that upgrade status is complete for each node in the second set:

system node upgrade-revert show -node nodename

The status should be listed as `complete`.

If the status is not successful for any node in the set, 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.

- c. Return to the admin privilege level:

set -privilege admin

12. Revert the LIFs back to the second set of nodes:

network interface revert *

Example

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

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

13. Verify that the nodes' data ports and LIFs are up and operational by completing the following steps for each node that was upgraded:

- a. Verify that the data ports for are up for each node:

```
network port show -node nodename -role data
```

Example

This example shows that all of a node's data ports are up.

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

Node	Port	Role	Link	MTU	Auto-Negot Admin/Oper	Duplex Admin/Oper	Speed (Mbps) Admin/Oper
node1	e0c	data	up	9000	true/true	full/full	auto/1000
	e0d	data	up	9000	true/true	full/full	auto/1000
	e1b	data	up	9000	true/true	full/full	auto/1000
	e1c	data	up	9000	true/true	full/half	auto/10
	e1d	data	up	9000	true/true	full/half	auto/10

5 entries were displayed.

- b. Verify that data LIFs successfully reverted back to each node in the first set, and that the LIFs are up:

```
network interface show -data-protocol nfs|cifs -role data -curr-node  
nodename
```

Example

This example shows that all of the data LIFs hosted by a node have successfully reverted back to the node, and that they are up.

```
cluster1:>> network interface show -data-protocol nfs|cifs -role data -curr-node node1
```

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	e0c	true
	data002	up/up	192.0.2.121/24	node0	e0d	true
	data003	up/up	192.0.2.122/24	node0	e0d	true
	data004	up/up	192.0.2.123/24	node0	e0c	true

4 entries were displayed.

14. If you previously determined that any of the partner nodes serve clients, verify that each node is providing service for each protocol that it was previously serving:

```
system node run -node nodename -command uptime
```

The operation counts reset to zero during the upgrade.

Example

This example shows that an upgraded 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
```

15. Trigger an AutoSupport notification by entering the following command for each node in the second set:

```
system node autosupport invoke -node nodename -type all -message
"finishing_NDU"
```

Verifying that the batch was upgraded successfully

After upgrading all of the nodes in a batch, you must verify that the target release is running on the nodes.

Steps

1. Confirm that the new Data ONTAP 8.2.x software is running on all of the nodes in the first batch:

```
system node image show
```

Example

This example of a 12-node cluster shows version 8.2.1 as the current version on the first batch of nodes (node0 - node5):

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

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	8.2.1	11/22/2013 13:52:22
	image2	false	false	8.1.2	10/25/2012 12:37:36
node1	image1	true	true	8.2.1	11/22/2013 13:52:22
	image2	false	false	8.1.2	10/25/2012 12:41:16
node2	image1	true	true	8.2.1	11/22/2013 13:52:22
	image2	false	false	8.1.2	10/25/2012 12:37:36
node3	image1	true	true	8.2.1	11/22/2013 13:52:22
	image2	false	false	8.1.2	10/25/2012 12:41:16
node4	image1	true	true	8.2.1	11/22/2013 13:52:22
	image2	false	false	8.1.2	10/25/2012 12:37:36
node5	image1	true	true	8.2.1	11/22/2013 13:52:22
	image2	false	false	8.1.2	10/25/2012 12:41:16
node6	image1	true	false	8.2.1	11/22/2013 13:52:22
	image2	false	true	8.1.2	10/25/2012 12:37:36
node7	image1	true	false	8.2.1	11/22/2013 13:52:22
	image2	false	true	8.1.2	10/25/2012 12:41:16
node8	image1	true	false	8.2.1	11/22/2013 13:52:22
	image2	false	true	8.1.2	10/25/2012 12:37:36
node9	image1	true	false	8.2.1	11/22/2013 13:52:22
	image2	false	true	8.1.2	10/25/2012 12:41:16
node10	image1	true	false	8.2.1	11/22/2013 13:52:22
	image2	false	true	8.1.2	10/25/2012 12:37:36

```
node11
      image1  true   false  8.2.1    11/22/2013 13:52:22
      image2  false  true   8.1.2    10/25/2012 12:41:16
12 entries were displayed.
```

- 2. Re-enable automatic giveback on the nodes if it was previously disabled by entering the following command on each node in the first batch:
- 3. Ensure that the cluster is in quorum and that services are running before upgrading the next batch of nodes.

You can use the `cluster show` and `cluster ring show` commands to verify that the cluster is in quorum.

After you finish

Upgrade the second batch by following the same steps that you used to upgrade the first batch. After both batches are upgraded, you should verify that the cluster was upgraded successfully.

Upgrading a Data ONTAP cluster disruptively

If you can take your cluster offline to upgrade to a new Data ONTAP release, or if you have a single-node cluster, you can use the disruptive upgrade method. This method has several steps: disabling storage failover for each HA pair, updating the software on each node in the cluster, and then reenabling storage failover.

Before you begin

You must have satisfied upgrade preparation requirements and verified that the cluster is ready to be upgraded.

About this task

During a disruptive upgrade, each node acts as a single-node cluster. Any failures in the node will cause a data outage.

Steps

- 1. Perform one of the following actions:

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

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

2. Reboot each node in the cluster:

```
system node reboot -node nodename
```

If the cluster consists of more than one node, you can reboot the nodes simultaneously.

Each node boots the new Data ONTAP image. The Data ONTAP login prompt appears, indicating that the reboot process is complete.

3. When each node has rebooted with the new Data ONTAP image, confirm that the new Data ONTAP 8.2.x software is running:

```
system node image show
```

Example

This example shows version 8.2.1 as the current version on both nodes:

```
cluster1::> system node image show
Node      Image  Is      Is      Current Version  Install
-----  -
node0     image1 true    true    8.2.1    11/22/2013 13:52:22
          image2 false   false   8.1.2    10/25/2012 12:37:36
node1     image1 true    true    8.2.1    11/22/2013 13:55:22
          image2 false   false   8.1.2    10/25/2012 12:41:16
4 entries were displayed.
```

4. Verify that the upgrade completed successfully for each node:

a. Set the privilege level to advanced:

```
set -privilege advanced
```

b. Ensure that upgrade status is complete for each node:

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

The status should be listed as complete.

If the status is not 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.

c. Return to the admin privilege level:

```
set -privilege admin
```

5. Enable storage failover for each HA pair in the cluster:

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

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

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

Completing post-upgrade tasks for cluster upgrades

After you upgrade a cluster to the latest version of Data ONTAP software, you must complete additional post-upgrade tasks.

Verifying the 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.

About this task

The cluster version is the lowest version of Data ONTAP running on any node in the cluster.

Step

1. Verify that the cluster version is the target Data ONTAP release:

```
version
```

Example

```
cluster1::> version
NetApp Release 8.2.1 Cluster-Mode: Fri Nov 22 23:37:32 PDT 2013
```

If the cluster version is not the target Data ONTAP release, run the `system node upgrade-revert upgrade` command to update the cluster version.

Verifying that the cluster is in quorum

Before and after you perform an upgrade, reversion, or downgrade, you must ensure that all nodes are participating in a replicated database (RDB) quorum and that all rings are in the quorum. You must also verify that the per-ring quorum master is the same for all nodes.

About this task

For more information about cluster replication rings and RDB quorums, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

Enter **y** to continue.

2. Display each RDB process:

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 vldb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.1.x:

```
cluster1::*> cluster ring show -unitname vldb
```

Node	UnitName	Epoch	DB Epoch	DB Trnxs	Master
node0	vldb	154	154	14847	node0
node1	vldb	154	154	14847	node0
node2	vldb	154	154	14847	node0
node3	vldb	154	154	14847	node0

4 entries were displayed.

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.2.x:

```
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.

For each process, verify the following configuration details:

- The relational database epoch and database epochs match for each node.
- The per-ring quorum master is the same for all nodes.
Note that each ring might have a different quorum master.

- Return to the admin privilege level:

```
set -privilege admin
```

- 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. During the upgrade, reversion, or downgrade process, each node will temporarily fall out of SAN quorum. Therefore, if you are verifying the SAN quorum after completing an upgrade, reversion, or downgrade, you may notice critical event messages warning you that the nodes were previously out of SAN quorum.

If a node is out of SAN quorum, you can use the `storage failover takeover` and `storage failover giveback` commands to perform a planned takeover and giveback with the node's high-availability partner and bring the node back into SAN quorum.

Example

In this example, both nodes in the cluster are in SAN quorum.

```
cluster1:> event log show -messagename scsiblade.*
Time           Node           Severity      Event
-----
8/13/2013 14:03:51 node0          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 14:03:51 node1          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
```

Example

This example shows a two-node cluster after performing an upgrade. Each node shows a previous out of SAN quorum event message from when the node was upgraded. However, the most recent event message for each node shows that both nodes are presently in SAN quorum.

```
cluster1:> event log show -messagename scsiblade.*
Time           Node           Severity      Event
-----
8/13/2013 15:37:51 node1          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:31:26 node1          CRITICAL      scsiblade.out.of.quorum: This node ...
8/13/2013 15:31:26 node1          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:31:26 node1          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:30:43 node0          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:24:16 node0          CRITICAL      scsiblade.out.of.quorum: This node ...
8/13/2013 15:24:16 node0          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:24:16 node0          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
```

Verifying cluster and SVM health

Before and after you upgrade, revert, or downgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and the aggregates and volumes are online.

Steps

- Verify that the nodes in the cluster are online and are eligible to participate in the cluster:

```
cluster show
```

Example

```
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. For more information about EMS messages, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

To troubleshoot cluster health issues, see the knowledgebase article [Troubleshooting Workflow: RDB app out of quorum](#) on the NetApp Support Site.

- Determine if any disk drives are broken, undergoing maintenance, or reconstructing:

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

- To verify that all aggregates are online, display the state of physical and logical storage, including storage aggregates:

```
storage aggregate show -state !online
```

This command displays the aggregates that are *not* online.

Example

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

For more information about managing aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide*.

- To verify that all volumes are online, display any volumes *not* online:

```
volume show -state !online
```

Example

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

For more information about managing volumes, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Enabling and reverting LIFs to home ports

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

About this task

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.

Steps

- 1. Display the status of all LIFs:

```
network interface show
```

Example

This example displays the status of all LIFs for a Storage Virtual Machine (SVM, formerly known as Vserver).

```
cluster1::> network interface show -vs0 vs0
Vserver      Logical   Status   Network   Current   Current   Is
-----
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
```


Example

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

3. Revert LIFs to their home ports:

```
network interface revert *
```

Example

This command reverts all LIFs back to their home ports and changes all LIF home statuses to true.

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

4. Verify that all LIFs are in their home ports:

```
network interface show
```

Example

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.
```

Creating a namespace mirror constituent for an upgraded Infinite Volume

After upgrading a cluster that contains an Infinite Volume, you must ensure that a namespace mirror constituent is created on all Infinite Volumes that span two or more nodes to provide data protection for the namespace constituent.

Before you begin

- An upgraded Infinite Volume must span two or more nodes to create a namespace mirror constituent.
- Determine whether to use this procedure or contact technical support.
 - If technical support created a data protection mirror copy for the namespace constituent in an Infinite Volume running Data ONTAP 8.1.x before you upgraded, you must contact technical

support after the upgrade to convert the data protection mirror copy of the namespace constituent to a namespace mirror constituent.

- If technical support did not create a data protection mirror copy for the namespace constituent in an Infinite Volume running Data ONTAP 8.1.x before you upgraded, you can use this procedure to create a namespace mirror constituent after the upgrade.

About this task

All the Infinite Volumes in a cluster running Data ONTAP 8.2 or later must have a namespace mirror constituent. An Infinite Volume that was upgraded from Data ONTAP 8.1.x does not have a namespace mirror constituent.

Note: When an Infinite Volume is in a data protection mirror relationship, only the source read/write Infinite Volume requires a namespace mirror constituent to provide data protection for the namespace constituent. The destination read-only Infinite Volume does not require a namespace mirror constituent because the data protection mirror relationship for the Infinite Volume provides data protection.

Steps

1. Ensure that the upgraded Infinite Volume has enough space for a namespace mirror constituent.
 - a. View the size of the namespace constituent on the Infinite Volume, and view the name of the aggregate that contains the namespace constituent by using the `volume show` command with the `-is-constituent true` parameter.

You need the size of the namespace constituent because the namespace mirror constituent will be the same size as the namespace constituent. You need the name of the aggregate because you must eliminate this aggregate from your evaluation. The namespace mirror constituent must be on a different aggregate than the namespace constituent, and the namespace mirror constituent should be on a different node than the namespace constituent.

Example

In the following example, the namespace constituent is named `repo_vol_ns`, and it is 10 TB in size. The name of the aggregate that contains the namespace constituent is `aggr_ns`.

```
cluster1::> volume show -is-constituent true
Vserver Volume                Aggregate State  Type Size  Available Used%
-----
vs0    repo_vol_default_data0001 aggr1    online RW   50TB   35.0TB  30%
vs0    repo_vol_default_data0002 aggr2    online RW   50TB   34.0TB  32%
vs0    repo_vol_default_data0003 aggr3    online RW   50TB   35.5TB  29%
vs0    repo_vol_default_data0004 aggr4    online RW   50TB   36.5TB  27%
vs0    repo_vol_ns                aggr_ns  online RW   10TB    8.4TB  16%
5 entries were displayed.
```

- b. In the cluster with the Infinite Volume, find an aggregate that is not on the same node as the aggregate that contains the namespace constituent by using the `aggregate show` command with the `-fields node` parameters.

Example

In the following example, the aggregate that contains the namespace constituent is named `aggr_ns`, and the aggregate is on node-02. You should not use any of the following aggregates on node-02: `aggr1` or `aggr_ns`. Instead you should use one of the following aggregates on node-01: `aggr2`, `aggr3`, or `aggr4`.

```
cluster1::> aggregate show -fields node
aggregate node
-----
aggr1      node-02
aggr2      node-01
aggr3      node-01
aggr4      node-01
aggr_ns    node-02
```

- c. Ensure one of the aggregates has enough space to fit the namespace mirror constituent.
- d. Increase aggregate space if required.

The Infinite Volume has enough space for the namespace mirror constituent.

2. Increase the size of the Infinite Volume by the size of the namespace constituent by using the `volume modify` command.

Example

In the following example, the volume named `repo_vol` is increased by the size of the namespace constituent, which is 10 TB:

```
cluster1::> volume modify -vserver vs0 -volume repo_vol -size +10TB
```

A namespace mirror constituent is automatically created.

Setting the cluster management LIF for Remote Support Agent

After you perform a Data ONTAP upgrade, if you use Remote Support Agent (RSA), you must use the `rsa setup` command on each remote management device to set the cluster management LIF for the RSA software.

About this task

For more information about configuring RSA and setting the cluster management LIF, see the *Remote Support Agent Configuration Guide for Clustered Data ONTAP*.

Resuming SnapMirror operations

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

Before you begin

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

Steps

1. Resume transfers for each SnapMirror relationship that was previously quiesced:
`snapmirror resume *`
2. Verify that the SnapMirror operations have resumed:
`snapmirror show`

Example

```
cluster1::> snapmirror show
```

Source Path	Type	Destination Path	Mirror State	Relationship Status	Total Progress	Healthy	Last 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".

After you finish

For each SnapMirror relationship that is configured to run on a schedule, you should verify that the first scheduled SnapMirror transfer completes successfully.

Upgrading older style data protection mirror relationships

Data protection mirror relationships that you have before upgrading to Data ONTAP 8.2 use a different relationship syntax and are not upgraded when you upgrade Data ONTAP. You must

upgrade relationship syntax style to Data ONTAP 8.2 syntax if you want to use new features and improvements.

About this task

After you upgrade a cluster, the cluster is fully operational with no disruption to existing services. However, data protection mirror relationships will not be able to take advantage of the new release's features because changing the syntax of the data protection mirror relationships from the Data ONTAP 8.1.x syntax to the Data ONTAP 8.2 syntax is not included in the upgrade.

Note: If you have data protection mirror relationships that span cluster peers, you must upgrade both destination and source clusters to clustered Data ONTAP 8.2 before upgrading older style data protection mirror relationships.

With Data ONTAP 8.2.1, conversion of 8.1.x style data protection mirror relationships to 8.2 style data protection mirror relationships will be initiated when you create a Storage Virtual Machine (SVM) peer relationship.

To take advantage of the new features, you must create an SVM peer relationship. Creating an SVM peer relationship automatically initiates the conversion of Data ONTAP 8.1.x style data protection mirror relationships to Data ONTAP 8.2 style data protection mirror relationships.

SVM peering requires unique SVM names. You should name SVMs with a unique fully qualified domain name (FQDN), for example, “dataVserver.HQ” or “mirrorVserver.Offsite”. Using the FQDN naming style makes it much easier to make sure of uniqueness.

Steps

1. Show the relationship-capability of the data protection mirror relationships by using the `snapmirror show` command with the `-fields relationship-capability` parameter.
2. Create SVM peer relationships:
 - a. On one of the clusters of the cluster peer relationship, create SVM peer relationships by using the `vserver peer create` command.

If you have more than one SnapMirror relationship that uses the same two SVMs, then you need to create only one SVM peer relationship.
 - b. On the other cluster of the cluster peer relationship, accept the SVM create request by using the `vserver peer accept` command.
 - c. If there is a name conflict, change the name of one of the SVMs by using the `vserver rename` command.

In addition to creating a SVM peer relationship, Data ONTAP upgrades the data protection mirror relationships to Data ONTAP 8.2 style relationships.

Note: Load-sharing mirror relationships cannot be upgraded to the Data ONTAP 8.2 style. The “Relationship capability” field of the detailed view of the `snapmirror show` command will show as “Pre 8.2”.

3. Ensure that all of the data protection mirror relationships are displayed as healthy and have relationship-capability of 8.2 and above by using the `snapmirror show` command with the `-instances` parameter.

Enabling automatic LIF rebalancing

If you previously disabled automatic LIF rebalancing to perform a batch upgrade, you should reenable it after completing the upgrade.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Enable automatic LIF rebalancing for each LIF as needed:

```
network interface modify -vserver Vserver_name -lif LIF_name -allow-lb-migrate true
```

3. Return to the admin privilege level:

```
set -privilege admin
```

Updating firmware

Because upgrading Data ONTAP includes upgrading your firmware, you must consider the requirements for upgrading system, disk, and disk shelf firmware, as well as firmware for other components that might be installed on your cluster. You might also need to update firmware between Data ONTAP upgrades.

How system firmware is updated during the Data ONTAP upgrade

When you perform a Data ONTAP software upgrade, the firmware service image included with the Data ONTAP upgrade package is copied to each node's boot device, and the new firmware is installed automatically.

If you are upgrading system firmware between Data ONTAP upgrades, you can obtain system firmware and information about how to install it from the NetApp Support Site.

Related information

System Firmware + Diagnostics Download: support.netapp.com/NOW/cgi-bin/fw

Disk firmware updates

Disk firmware is bundled with the Data ONTAP upgrade package and updated automatically during Data ONTAP upgrades. You can also obtain disk firmware from the NetApp Support Site and update it manually.

Related information

Disk Drive and Firmware Matrix: support.netapp.com/NOW/download/tools/diskfw

How disk firmware is updated

When you upgrade Data ONTAP, disk firmware is updated automatically if the firmware on the disks is older than the firmware that is bundled with the Data ONTAP upgrade package. You can also update disk firmware by downloading the most recent firmware package from the NetApp Support Site and installing the files.

Each node is shipped with the latest firmware revisions. Disk firmware is updated automatically when one of the following is true:

- You add new disks or a disk shelf.
Disk firmware updates are applied from any firmware bundle resident on the node.

Note: When hot-adding SAS shelves, firmware is not updated automatically. You must manually check and update out-of-date drive, shelf, and ACP firmware.

- Data ONTAP detects disk firmware updates on the node.
Data ONTAP scans for new firmware every two minutes.

Disk firmware updates can be added to the node at the following times:

- During a Data ONTAP upgrade
Disk firmware updates are often included with an upgrade to a new release family. Disk firmware updates are occasionally included in Data ONTAP upgrades within release families.
- After obtaining a disk firmware update package
You might be directed to download a disk firmware update from the NetApp Support Site if you encounter problems with certain disk types or you receive a notice from NetApp.
You must download and install the latest disk firmware before upgrading Data ONTAP.
- When you hot-add a SAS shelf

Each disk drive manufacturer has its own disk drive firmware. Therefore, disk firmware updates can include updates to firmware for one or more disk drive types. Because your cluster might use drives from multiple drive manufacturers, whether you are affected by a disk firmware update depends on the types and numbers of drives on your system.

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 can obtain the DQP from the NetApp Support Site. 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

Related information

Disk Qualification Package Instructions: support.netapp.com/NOW/download/tools/diskqual

Disk Drive & Firmware Matrix: support.netapp.com/NOW/download/tools/diskfw

Service availability during disk firmware updates

By default, disk firmware updates take place automatically in the background so as to ensure the continuity of cluster services.

You can download the disk firmware package to your cluster at any time and the firmware is updated nondisruptively in the background. However, you must wait until the disk firmware update has finished before initiating a nondisruptive upgrade.

Background disk firmware updates take place one disk at a time and require approximately 2.5 minutes per disk. Although it is not likely that all the disks attached to your cluster would need firmware updates at the same time, it is a best practice to wait at least 2.5 minutes for every disk attached to a node before proceeding with a Data ONTAP NDU.

For example, if a node has 192 disks attached, you should wait at least 480 minutes, or 8 hours. You should wait until all nodes in the cluster have completed the firmware update before proceeding with the NDU. Disk firmware can be updated in parallel on all nodes in a cluster.

Detecting outdated disk firmware using AutoSupport

AutoSupport messages include information about disk firmware installed on your cluster. The Installed Systems pages use these messages to monitor the firmware versions on your cluster and to post notices when installed disk firmware on your cluster has been superseded.

Before you begin

To use the Installed Systems service to monitor disk firmware versions, your cluster must meet the following requirements:

- AutoSupport must be already enabled on your cluster.
For more information about AutoSupport, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.
- You must have registered your NetApp products.

Steps

1. Use a web browser to go to the NetApp Support Site at support.netapp.com.
2. Select **My Support > View Installed Systems**.
3. Display the product details for the cluster you are upgrading by entering search criteria for a specific cluster or displaying a list of clusters at your company.
4. In the AutoSupport Status category, click **Health Check Details**.

Result

If a firmware update is available for your cluster, you see a message with a link to a Firmware Analysis page. If the Firmware Analysis page contains a message that newer disk firmware is

available for your cluster, a disk firmware update takes place during your next Data ONTAP upgrade. If there is no disk firmware message, the disk firmware on your cluster is up-to-date.

Related information

Systems: support.netapp.com/eservice/Systems.jsp

Disk shelf firmware updates

Disk shelf firmware (firmware for modules on disk shelves) is bundled with the Data ONTAP upgrade package and updated automatically during Data ONTAP upgrades. You can also obtain disk shelf firmware from the NetApp Support Site and update it manually.

Disk shelf firmware updates are mandatory when hot-adding a disk shelf. See your disk shelf documentation for more information.

Related information

Disk shelf firmware: support.netapp.com/NOW/download/tools/diskshelf

How disk shelf firmware is updated

When you upgrade Data ONTAP, disk shelf firmware is updated automatically if the firmware on the shelves is older than the firmware that is bundled with the Data ONTAP upgrade package. You can also update disk shelf firmware by downloading and installing the most recent firmware for your shelf modules from the NetApp Support Site.

The AT series, ESH series, and SAS shelf I/O module (IOM) series in a disk shelf provide for the connection of the disks to the host bus adapter interface, including signal integrity when disks are swapped. There are two modules in the middle of the rear of the disk shelf, one for Channel A and one for Channel B. SAS modules can also be internal components in certain systems. Updated firmware for these modules is made available periodically.

Each node is shipped with the latest disk shelf firmware versions.

Disk shelf firmware updates can be loaded onto the cluster at the following times:

- After a Data ONTAP upgrade
Disk shelf firmware updates are often included in Data ONTAP upgrade packages. After the Data ONTAP upgrade process is completed on each node in an HA pair, if the new disk shelf firmware version is later than the installed version, the new version is downloaded and installed on the disk shelves attached to both nodes in the HA pair.
- During a manual firmware update
You might need to download a disk shelf firmware update from the NetApp Support Site if you plan to perform a nondisruptive upgrade of Data ONTAP software, or if you receive a notice from NetApp.
- When you hot-add a SAS shelf

The following events can also trigger an automatic disk shelf firmware update when there is new firmware on the cluster:

- The `system reboot` command is issued.
- The `storage failover giveback` command is issued.
- New disk drives are inserted.
- New shelf modules are inserted.

For more information about disk shelves and disk shelf modules, see the *Clustered Data ONTAP High-Availability Configuration Guide* and the *Installation and Service Guide* for your shelves.

Detecting outdated disk shelf firmware

If you want to perform a nondisruptive upgrade of Data ONTAP software, or if you are directed to update disk shelf firmware, you must first determine which firmware version is installed on disk shelves attached to your cluster.

Steps

1. Go to the disk shelf firmware information on the NetApp Support Site and determine the most recent firmware version for your shelves.
2. At the clustershell, enter the following command:
`system node run nodename sysconfig -v`
3. Locate the shelf information in the `sysconfig -v` output:

Example

```
Shelf 1: DS4143 Firmware rev. IOM3 A: 0110 IOM3 B: 0110
Shelf 2: DS14-MK2-AT Firmware rev. AT-FCX A: 36 AT-FCX B: 36
```

If the disk shelf firmware version in the command output is earlier than the most recent version on the NetApp Support Site, you must update your disk shelf firmware manually.

Related information

Disk Shelf Firmware: support.netapp.com/NOW/download/tools/diskshelf

How ACP firmware is updated

If your disk shelves include ACP functionality, ACP firmware is updated automatically during Data ONTAP upgrades. You can also obtain it from the NetApp Support Site and update it manually.

When you upgrade Data ONTAP, ACP firmware (firmware for ACP processors on disk shelves) is updated automatically if the firmware in the ACP processors is older than the firmware that is bundled with the Data ONTAP upgrade package.

Related information

Disk Shelf Firmware: support.netapp.com/NOW/download/tools/diskshelf

Instructions for Downloading and Installing Disk Shelf Firmware on Data ONTAP Cluster-Mode: support.netapp.com/NOW/download/tools/diskshelf/shelffw_cm.html

Service Processor firmware updates

Service Processor (SP) is a remote management device that is included in some clusters. Starting with Data ONTAP 8.2, a baseline SP firmware image is packaged with the Data ONTAP upgrade package, so that the SP is updated automatically by default.

Any existing connection to the SP is terminated when the SP firmware is being updated. This is the case whether the SP firmware update is automatic or manually triggered.

Note: Data ONTAP detects a failed SP automatic update and triggers a corrective action to retry the SP automatic update up to three times. If all three retries have failed, you should contact technical support.

If you are upgrading SP firmware between Data ONTAP upgrades, you can obtain SP firmware and information about how to install it from the NetApp Support Site. You can download and update the SP firmware by using the Data ONTAP CLI or the SP CLI.

For information about what the SP is and how it works, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

RLM firmware updates

You can upgrade the Remote LAN Module (RLM) firmware by downloading and updating the RLM firmware using the Data ONTAP CLI or the RLM CLI.

You can obtain RLM firmware and information about how to install it from the NetApp Support Site.

For information about what the RLM is and how it works, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

How Flash Cache firmware is updated

Firmware for Flash Cache devices is included with the upgrade package for Data ONTAP upgrades. If the running firmware is older than the firmware that is bundled with the Data ONTAP upgrade package, it is updated automatically.

Firmware updates are not available for the original 16-GB PAM devices. Automatic updates occur only to Flash Cache devices, not PAM devices.

If you are upgrading Data ONTAP nondisruptively (NDU), Flash Cache firmware is updated nondisruptively. This is because the reboot required for Flash Cache firmware upgrades occurs before the final reboot of the `storage failover giveback` process. Consequently, if your cluster includes Flash Cache devices, you might see multiple reboots during a Data ONTAP NDU; this is expected behavior.

For information about what Flash Cache and PAM are and how they work, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Reverting clusters to an earlier Data ONTAP release family

Transitioning a cluster to a release in an earlier Data ONTAP family is referred to as a *reversion*. Reverting requires preparation, using the `system node revert-to` command in the clustershell, using the `revert_to` command in the nodeshell, and completing post-reversion procedures.

The `revert_to` command modifies Data ONTAP on-disk structures to be compatible with the earlier target release and ensures that the cluster is prepared for the reversion.

Attention: *Do not* attempt to revert Data ONTAP by simply downloading and booting (or netbooting) a release in an earlier release family. If you do, you cannot boot the earlier target release. You must use the clustershell `system node revert-to` and nodeshell `revert_to` commands for the reversion process.

For more information, see the `system node revert-to` man page.

When to revert and when to call technical support

You can revert without assistance when reverting new or test clusters, but you should call technical support if you encounter problems during or after upgrading, or if you want to revert a production cluster.

You can revert to an earlier release family without assistance from technical support only in the following scenarios:

- You upgraded to a new release on a test cluster and you want to return to the original release when testing is completed.
- You are configuring a new cluster—running a later release of Data ONTAP and not yet in production—in an environment in which you have standardized on an earlier Data ONTAP release.

Do not attempt to revert Data ONTAP in a production environment without assistance. If you encounter any of the following circumstances, contact technical support immediately:

- The upgrade process fails and cannot finish.
- The upgrade process finishes, but the cluster is unusable in a production environment.
- The upgrade process finishes and the cluster goes into production, but you are not satisfied with its behavior.
- The upgrade process finishes for some but not all of the nodes, and you decide that you want to revert.

Planning your reversion

Because new features are introduced in each release of Data ONTAP, you must understand reversion requirements and evaluate how they might impact your current configuration.

Before proceeding with the reversion, you should do the following:

- Review the *Release Notes* for the Data ONTAP reversion source release.
- Understand any requirements for reverting to the target release from your existing software.
- Note any potential functionality changes to your cluster after the reversion.
- Prepare to address all points in the reversion checklist.

Cluster reversion checklist

You can use this checklist to record your progress as you prepare for the reversion, perform the reversion, and complete post-reversion tasks.

Steps for preparing to revert

Preparatory steps are complete when all of the following conditions are true:

Condition	Complete?
Software and hardware support in the target release is confirmed. To confirm hardware support, visit <i>Hardware Universe</i> at hww.netapp.com If any nodes are platforms that are not supported in the target release, then you should unjoin the nodes from the cluster before you revert the cluster. For more information about removing nodes from a cluster, see the <i>Clustered Data ONTAP System Administration Guide for Cluster Administrators</i> .	
The SAN configuration is fully supported. You must verify that your SAN configuration does not exceed the limits for the target Data ONTAP release. For more information about SAN configuration limits, see the <i>Clustered Data ONTAP SAN Configuration Guide</i> .	
All release-specific reversion issues have been resolved.	
You have access to the clustershell at the advanced privilege level.	

Condition	Complete?
<p>The cluster and Storage Virtual Machines (SVMs) are running and healthy.</p> <p>All aggregates and volumes should be healthy and online before proceeding with the reversion. You can use the <code>cluster show</code> command to verify the status of the nodes.</p>	
<p>The cluster is in quorum.</p> <p>All nodes are participating in a quorum and all rings are in the quorum. The per-ring quorum master should be the same for all nodes.</p>	
<p>All core dump files have been either saved or deleted.</p> <p>For more information about managing core dumps, see the <i>Clustered Data ONTAP System Administration Guide for Cluster Administrators</i>.</p>	
<p>The system time is synchronized across the cluster.</p>	
<p>The iSNS server and its associated SVM management LIF are configured with IPv4 addresses.</p>	
<p>Snapshot copies created in the later Data ONTAP release have been deleted, and all Snapshot copies from the nodes' root volumes and root aggregates have been deleted.</p> <p>You must delete any Snapshot copies that were created after upgrading to the current release, delete root aggregate and root volume Snapshot copies, and disable Snapshot schedules for the root aggregate and root volume.</p>	
<p>All IPv6 objects have been deleted.</p> <p>You must delete all LIFs, routing groups, and firewall policies that use IPv6 addresses. For more information about deleting these objects, see the <i>Clustered Data ONTAP Network Management Guide</i>.</p>	
<p>You have the target Data ONTAP software image available on an HTTP server.</p> <p>Download the software image for the target Data ONTAP release from the NetApp Support Site at support.netapp.com, and place it on an HTTP server that is accessible by each node.</p>	

Condition	Complete?
<p>The target Data ONTAP software images are installed on each node and set as the alternate boot device image.</p> <p>You can use the <code>system node image update</code> command to install the software images. You can use the <code>system node image show</code> command to verify that the software images are installed as the alternate boot image on each node.</p>	

Steps for performing the reversion

The reversion is complete when all of the following steps have been completed:

Condition	Complete?
<p>No jobs are running.</p> <p>If any aggregate, volume, mirror, NDMP (dump or restore), or Snapshot jobs (such as create, delete, move, modify, replicate, and mount jobs) are running or queued, allow the jobs to complete successfully or stop the queued entries.</p>	
<p>The target Data ONTAP software is installed and set as the default boot image.</p>	
<p>Each node has booted the target release.</p>	

Steps for after reverting

Post-reversion steps are complete when all of the following conditions are true:

Condition	Complete?
<p>The cluster and SVMs are running and healthy.</p> <p>All aggregates and volumes should be healthy and online after the reversion. You can use the <code>cluster show</code> command to verify the status of the nodes.</p>	
<p>LIFs are online and on their correct home ports.</p> <p>You can use the <code>network interface</code> command to display and modify LIF configuration.</p>	
<p>Snapshot schedules are enabled for each node's root volume and root aggregate.</p> <p>You must enable Snapshot schedules of the root volume and root aggregate to start creating Snapshot copies again.</p>	

Condition	Complete?
Client access is verified. You should verify that clients can access the cluster for each configured protocol.	
The Service Processor firmware version is confirmed. If your current SP firmware version is not supported for the Data ONTAP release to which you reverted, you must install a supported SP firmware version for the earlier Data ONTAP release.	
The event generate-autosupport-log capability is enabled for the SVM administrator vsadmin role.	

Reversion process considerations

Make sure that you know about revert issues and limitations before beginning a Data ONTAP reversion.

Be aware of the following issues:

- Clusters consisting of more than one node can be reverted from Data ONTAP 8.2.x to 8.1.x. Single node clusters cannot be reverted to Data ONTAP 8.1.
- If the cluster contains a Storage Virtual Machine (SVM) with Infinite Volume, do not attempt to revert to Data ONTAP 8.1.
If you are reverting to Data ONTAP 8.1.1 or a later release of Data ONTAP 8.1.x, you should contact technical support for assistance. If you are reverting to Data ONTAP 8.1.0, you must delete all SVMs with Infinite Volume.
- Reversion is disruptive.
No client access can occur during the reversion. If you are reverting a production cluster, be sure to include this disruption in your planning.
- Reversion affects all nodes in the cluster.
The reversion must be performed on all nodes in the cluster; however, some of the procedures must be performed on each HA pair and completed on each set of nodes before other pairs are reverted.
- The reversion is complete when all nodes are running the new target release.
When the cluster is in a mixed-version state, you should not enter any commands that alter the cluster operation or configuration except as necessary to satisfy reversion requirements; monitoring operations are permitted.
If you are unable to complete the reversion for any reason, contact technical support immediately. If you have reverted some, but not all, of the nodes, do not attempt to upgrade the cluster back to the source release.
- You might notice reduced performance for client operations.
Storage QoS, which prioritizes client and system operations, is not available when you revert from Data ONTAP 8.2 to 8.1.x.

- When you revert a node, it clears the cached data in a Flash Cache module.
Because there is no cached data in the Flash Cache module, the node serves initial read requests from disk, which results in decreased read performance during this period. The node repopulates the cache as it serves read requests.
- When you revert a volume containing FlexCache volumes from Data ONTAP 8.2 to Data ONTAP 8.1.x, the FlexCache volumes are not deleted.
The FlexCache volumes become dormant and cannot be used for caching read requests from clients.
- After you enter the `system node revert-to` command to revert a cluster, the `version` command becomes unavailable and does not display any output until the reversion is completed.

Identifying potential reversion issues

Every Data ONTAP release family has unique reversion requirements that you must understand and resolve before you decide to revert.

For additional information, and to check for reversion issues that might have been discovered later, see the *Clustered Data ONTAP Release Notes*. The following list summarizes reversion issues known when this guide was published.

- If you gained access to licensed or entitled features by upgrading to Data ONTAP 8.2 or later and these features required a license prior to Data ONTAP 8.2, you might need to install a license after reverting.
This is the case if a license was not previously installed for the release to which you revert.
- You need to be aware of the licensing implications if you have a node that is shipped with Data ONTAP 8.2 and you want to revert it to a release in the Data ONTAP 8.1 release family.
If your system is shipped with Data ONTAP 8.2 or later and you reinstall it with a release in the Data ONTAP 8.1 release family, you must install a key for the desired license package in the format supported by the Data ONTAP 8.1 release family.
- If your current SP firmware version is not supported for the Data ONTAP release to which you are downgrading or reverting, you must install a supported SP firmware version for the earlier Data ONTAP release.
- Support for up to 1,024 ACEs in NFSv4 ACLs is a new feature in Data ONTAP 8.2.
Reverting to a previous release family requires action if you have NFSv4 ACLs in your environment that contain more than 400 ACEs.
- Before reverting to a release earlier than Data ONTAP 8.2.1, you must ensure that off-board antivirus is disabled on all the nodes within a cluster.
If you do not disable off-board antivirus on all the nodes, you will not be able to revert to an earlier release.
- If you downgrade or revert to a release earlier than Data ONTAP 8.2.1, you must run the `security ssh prepare-to-downgrade` command at the advanced privilege level to reset the SSH security configurations of the cluster and all Storage Virtual Machines (SVMs) to the default settings used in the earlier release.
- Exporting qtrees is not supported in releases earlier than Data ONTAP 8.2.1.

If you plan to downgrade or revert to an earlier release, you must first take certain actions; otherwise, the downgrade or revert operation fails.

- Starting with Data ONTAP 8.2, NTP is always enabled.
If you revert to an earlier release, NTP remains enabled regardless of the prior setting for NTP when you were running the earlier release.
- Before reverting to a release earlier than Data ONTAP 8.2, you must remove the non-server types of digital certificates and the user logins that have the `cert` authentication method.
- If you revert to Data ONTAP 8.1.2 or earlier, Data ONTAP prompts you to run the `security login role config reset` command to reset some role-based access control (RBAC) characteristics to their default values.
- RSH and IPv6 connections are supported only for Data ONTAP 8.2 and later releases.
Before reverting to an earlier release, you must manually remove RSH user accounts and the IPv6 firewall policies that were added for enabling clear-text protocols (RSH and Telnet).
- AD domain users' access to the cluster is supported only on Data ONTAP 8.1.1 and later releases.
If you revert to an earlier release, Data ONTAP prompts you to delete any existing authentication tunnel that is used for authenticating AD domain users' cluster access.

Preparing to revert Data ONTAP clusters

Before reverting to an earlier Data ONTAP release family, you must verify reversion requirements, resolve any reversion issues, and obtain the Data ONTAP software image for the target release.

Be sure to check the *Release Notes* for this Data ONTAP source release for any updates to reversion notices and procedures.

Verifying that the cluster is in quorum

Before and after you perform an upgrade, reversion, or downgrade, you must ensure that all nodes are participating in a replicated database (RDB) quorum and that all rings are in the quorum. You must also verify that the per-ring quorum master is the same for all nodes.

About this task

For more information about cluster replication rings and RDB quorums, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

Enter `y` to continue.

2. Display each RDB process:

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 vldb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.1.x:

```
cluster1::*> cluster ring show -unitname vldb
```

Node	UnitName	Epoch	DB Epoch	DB Trnxs	Master
node0	vldb	154	154	14847	node0
node1	vldb	154	154	14847	node0
node2	vldb	154	154	14847	node0
node3	vldb	154	154	14847	node0

4 entries were displayed.

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.2.x:

```
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.

For each process, verify the following configuration details:

- The relational database epoch and database epochs match for each node.
- The per-ring quorum master is the same for all nodes.

Note that each ring might have a different quorum master.

3. Return to the admin privilege level:

```
set -privilege admin
```

4. 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. During the upgrade, reversion, or downgrade process, each node will temporarily fall out

of SAN quorum. Therefore, if you are verifying the SAN quorum after completing an upgrade, reversion, or downgrade, you may notice critical event messages warning you that the nodes were previously out of SAN quorum.

If a node is out of SAN quorum, you can use the `storage failover takeover` and `storage failover giveback` commands to perform a planned takeover and giveback with the node's high-availability partner and bring the node back into SAN quorum.

Example

In this example, both nodes in the cluster are in SAN quorum.

```
cluster1:> event log show -messagename scsiblade.*
Time           Node           Severity      Event
-----
8/13/2013 14:03:51 node0          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 14:03:51 node1          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
```

Example

This example shows a two-node cluster after performing an upgrade. Each node shows a previous out of SAN quorum event message from when the node was upgraded. However, the most recent event message for each node shows that both nodes are presently in SAN quorum.

```
cluster1:> event log show -messagename scsiblade.*
Time           Node           Severity      Event
-----
8/13/2013 15:37:51 node1          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:31:26 node1          CRITICAL      scsiblade.out.of.quorum: This node ...
8/13/2013 15:31:26 node1          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:31:26 node1          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:30:43 node0          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:24:16 node0          CRITICAL      scsiblade.out.of.quorum: This node ...
8/13/2013 15:24:16 node0          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:24:16 node0          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
```

Verifying cluster and SVM health

Before and after you upgrade, revert, or downgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and the aggregates and volumes are online.

Steps

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster:

cluster show

Example

```
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. For more information about EMS messages, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

To troubleshoot cluster health issues, see the knowledgebase article [Troubleshooting Workflow: RDB app out of quorum](#) on the NetApp Support Site.

2. Determine if any disk drives are broken, undergoing maintenance, or reconstructing:

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

3. To verify that all aggregates are online, display the state of physical and logical storage, including storage aggregates:

```
storage aggregate show -state !online
```

This command displays the aggregates that are *not* online.

Example

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

For more information about managing aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide*.

4. To verify that all volumes are online, display any volumes *not* online:

```
volume show -state !online
```

Example

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

For more information about managing volumes, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Preparing to revert production clusters

If you are reverting a cluster that you have configured to serve data to clients in your environment, you must ensure that certain configurations are prepared for the reversion.

Ending SnapMirror and SnapVault relationships before reverting

When you revert a cluster, you must end SnapMirror and SnapVault relationships before reverting. Depending on the compatibility type of the relationship or the kind of relationship it is, you might have to delete SnapMirror relationships, Storage Virtual Machine (SVM) peer relationships, and possibly cluster peer relationships.

The following lists what you must do to prepare SnapMirror and SnapVault relationships before reverting a cluster:

- Load-sharing mirror relationships
You must delete all load-sharing mirror relationships and load-sharing mirror destination volumes.
- Data protection mirror relationships
You must delete all data protection mirror relationships that are compatible with Data ONTAP 8.2 because they are not compatible with Data ONTAP 8.1.
- SnapVault relationships
You must delete all SnapVault relationships because they do not exist prior to Data ONTAP 8.2.
- SVM peer relationships
You must delete all SVM peer relationships because they do not exist prior to Data ONTAP 8.2.
- Cluster peer relationships
After deleting all the previously listed relationships, you can try to revert the operating system without deleting cluster peer relationships. If any cluster peer relationships do need to be deleted, you are notified during the revert process.

Deleting load-sharing and data protection mirror relationships before reverting

Before reverting to Data ONTAP 8.1.x, you must delete all load-sharing mirror relationships and any data protection mirror relationships that were created in Data ONTAP 8.2.

Steps

1. View and save information about all of your mirror relationships and each relationship's destination volume by using the `snapmirror show` command and `volume show` commands, respectively.

The following mirror relationships must be deleted:

- All load-sharing mirror relationships
- Any data protection mirror relationships that were created in Data ONTAP 8.2
When viewing mirror relationships by using the `snapmirror show` command, these relationships have a `relationship capability` of 8.2 and above.

- All data protection relationships if the cluster was re-created in Data ONTAP 8.2
If the cluster was re-created in Data ONTAP 8.2 by using the `system configuration recovery cluster recreate` command, then all data protection relationships must be deleted.

Example

This example identifies the relationship capability of the mirror relationships in the cluster:

```
cluster1::> snapmirror show -fields relationship-capability
source-path destination-path relationship-capability
-----
vs1:vol1    vs1:vol3          "8.2 and above"
```

2. Break each data protection relationship that you identified by using the `snapmirror break` command.

Example

```
cluster1::> snapmirror break -destination-path vs1:vol3
```

3. Delete each data protection mirror and load-sharing mirror relationship that you identified by using the `snapmirror delete` command.

Example

```
cluster1::> snapmirror delete -destination-path vs1:vol3
```

Only the mirror relationships are deleted; the destination volumes remain.

4. For each data protection mirror relationship that you deleted, use the `snapmirror release` command from the source node to remove the configuration information and snapshot copies from the source volume.

Example

```
cluster1::> snapmirror release -relationship-info-only -source-path vs1:vol1 -destination-path vs1:vol3
```

5. Take each load-sharing destination volume offline by using the `volume offline` command.
6. Delete each load-sharing and uninitialized data protection destination volume by using the `volume delete` command.

After you finish

If desired, re-create the mirror relationships in the target reversion release.

Deleting data protection mirror relationships before reverting

Before reverting to Data ONTAP 8.1.x, you must break and delete any data protection mirror relationships that has the relationship capability of “8.2 and above” and you must break data protection mirror relationships with a relationship capability of “Pre-8.2.”

About this task

The extent of what you must do with data protection mirror relationships before reverting the cluster depends on whether the data protection mirror relationships have a relationship capability of “8.2 and above”:

- If the relationships have a relationship capability of “Pre-8.2,” you must release source volumes for relationships whose source volumes reside on the cluster you are reverting, and you must break relationships whose destination volumes reside on the cluster you are reverting. You do not need to do anything on cluster peers that have either source or destination volumes for the data protection mirror relationships you broke or released.
- If the relationships have a relationship capability of “8.2 or above,” you must remove the data protection mirror relationship entirely by releasing source volumes and by breaking and deleting destination volumes on the cluster you are reverting and on cluster peers.

The following procedure performs the tasks on the cluster you are reverting first, then performs tasks on the cluster peers. There are three clusters configured with a data protection mirror between cluster peers “cluster1” and “cluster2”, and a data protection mirror between cluster peers “cluster2” and “cluster3”. The procedure uses examples that describe the process for data protection mirror relationships that have a relationship capability of “8.2 or above.”

Steps

1. On the cluster you are reverting, remove data protection mirror relationships whose destination volumes are on the cluster and release source volumes on the cluster.
 - a. On the cluster you are reverting, view information about the relationship capability of your mirror relationships by using the `snapmirror show` command with the `-fields relationship-capability` parameter.

Example

This example identifies the relationship capability of the mirror relationships in the cluster:

```
cluster2:> snapmirror show -fields relationship-capability
source-path destination-path relationship-capability
-----
c1l1vs1:vol1 c1l2vs2:vol2      "8.2 and above"
```

- b. Break each identified data protection mirror relationship by using the `snapmirror break` command.

Example

```
cluster2:> snapmirror break -destination-path cl2vs2:vol2
```

- c. Delete each identified data protection mirror relationship by using the `snapmirror delete` command.

Example

```
cluster2:> snapmirror delete -destination-path cl2vs2:vol2
```

Only the mirror relationships are deleted; the destination volumes remain.

- d. List any relationships that have source volumes on the cluster you are reverting by using the `snapmirror list-destinations` command.

Example

```
ie3070:> snapmirror list-destinations
```

Source Relationship Path	Destination Type Path	Transfer Status	Progress Progress	Progress Last Updated	Id
cl2vs2:vol2	DP cl3vs3:vol3	-	-	-	590f2d55-fb9e-11e2-b2fc-123478912345

- e. Remove the configuration information and Snapshot copies from the data protection mirror relationship whose source is on the cluster you are reverting by using the `snapmirror release` command.

Example

```
cluster2:> snapmirror release -relationship-info-only -source-path cl2vs2:vol2
-destination-path cl3vs3:vol3
```

2. On cluster peers that have either source volumes or destination volumes that are endpoints of relationships you previously broke and deleted or released, complete the removal of the relationships by removing or releasing the relationships on the cluster peers.
 - a. Using the destination volume information from step 1d, list the relationship compatibility by using the `snapmirror show` command with the `-fields relationship-compatibility` parameter.

Example

```
cluster3:> snapmirror show -fields relationship-compatibility
source-path destination-path relationship-compatibility
-----
```

```
cl2vs2:vol2 cl3vs3:vol3 "8.2 and above"
```

- b. Break the relationship shown by the `snapmirror show` command by using the `snapmirror break` command on the cluster that contains the destination volume.

Example

```
cluster3::> snapmirror break -destination-path cl3vs3:vol3
```

- c. Delete the relationship shown by the `snapmirror show` command by using the `snapmirror delete` command on the cluster that contains the destination volume.

Example

```
cluster3::> snapmirror delete -destination-path cl3vs3:vol3
```

- d. Remove the configuration information and Snapshot copies by using the `snapmirror release` command on the cluster that contains the source volume.

This relationship is shown by the `snapmirror show` command of Step 1a.

Example

```
cluster1::> snapmirror release -relationship-info-only -source-path cl1vs1:vol1
-destination-path cl2vs2:vol2
```

After you finish

If desired, re-create the mirror relationships in the target reversion release.

Deleting SnapVault relationships before reverting

Before reverting to Data ONTAP 8.1.x, you must delete all SnapVault relationships that were created in Data ONTAP 8.2. The ability to back up a volume using SnapVault technology did not exist before Data ONTAP 8.2.

Steps

1. View and save information about all of your SnapVault relationships by using the `snapmirror show` command.

Example

```
cluster1::> snapmirror show
```

Source Path	Type	Destination Path	Mirror State	Relationship Status	Total Progress	Progress Last Healthy	Updated
vs1:vol2	XDP	vs1:vol2_backup					

Snapmirrored			
idle	-	true	-

2. Change the privilege level of the command session to advanced by using the `set` command with the `-privilege advanced` parameter.
3. Break each SnapVault relationship that you identified by using the `snapmirror break` command with the `-delete-snapshots` parameter.

Using the `-delete-snapshots` parameter deletes all of the Snapshot copies on the volume, a prerequisite for reverting if you have SnapVault relationships.

Example

```
cluster1::*> snapmirror break -destination-path vs1:vol2_backup
-delete-snapshots
```

4. Delete each SnapVault relationship that you identified by using the `snapmirror delete` command.

Example

```
cluster1::*> snapmirror delete -destination-path vs1:vol2_backup
```

Only the SnapVault relationships are deleted; the destination volumes remain.

5. For each SnapVault relationship that you deleted, use the `snapmirror release` command from the source volume to remove the configuration information and Snapshot copies from the source volume.

Example

```
cluster1::*> snapmirror release -source-path vs1:vol2 -destination-path vs1:vol2_backup
```

6. Take each destination volume offline by using the `volume offline` command.
7. Delete each destination volume by using the `volume delete` command.

Deleting SVM peer relationships before reverting

Before reverting to Data ONTAP 8.1.x, you must delete Storage Virtual Machine (SVM) peer relationships created in Data ONTAP 8.2 because they did not exist in Data ONTAP 8.1.x.

Before you begin

SnapMirror relationships must be deleted. The topic “Deleting data protection mirror relationships before reverting” contains detailed instructions.

Steps

1. Ensure that there are no SnapMirror relationships involving the cluster you are reverting by using the `snapmirror show` command.

Example

```
cluster2::> snapmirror show
This table is currently empty.
```

2. To determine the SVM peer relationships you want to delete, view the SVM peer relationships on the cluster you are reverting by using the `vserver peer show` command.

Example

```
cluster2::> vserver peer show
      Vserver      Peer      Peer
      Vserver      Vserver    State
-----
cl1vs1      cl2vs2
peered
cl2vs2      cl3vs3
peered

3 entries were displayed.
```

3. Delete each SVM peer relationship by using the `vserver peer delete` command.

Example

```
cluster2::> vserver peer delete -vserver cl1vs1
-peer-vserver cl2vs2
cluster2::> vserver peer delete -vserver cl2vs2
-peer-vserver cl3vs3
```

Deleting cluster peer relationships before reverting

Before reverting to Data ONTAP 8.1.x, you might have to delete cluster peer relationships created or modified in Data ONTAP 8.2 because they are not compatible with the Data ONTAP 8.1.x format.

Before you begin

- All SnapMirror relationships must be deleted.
- All Storage Virtual Machine (SVM) peer relationships must be deleted.

About this task

Typically, you do not have to delete cluster peer relationships when reverting, but there are some cases in which you do have to delete cluster peer relationships. If deleting cluster peer relationships is required, a Data ONTAP 8.2 message notifies you to delete all SnapMirror relationships and cluster peer relationships after you initiate the cluster revert process by using the `system node revert-to` command.

Steps

1. Ensure that there are no SnapMirror relationships involving the cluster you are reverting by using the `snapmirror show` command.

Example

This example shows that there are no SnapMirror relationships.

```
cluster2::> snapmirror show
This table is currently empty.
```

2. Ensure that there are no SVM peer relationships configured on the cluster you are reverting by using the `vserver peer show` command.

Example

```
cluster2::> vserver peer show
There are no Vserver peer relationships.
```

3. Show all of the configured cluster peer relationships by using the `cluster peer show` command.

Example

```
cluster2::> cluster peer show
Peer Cluster Name      Cluster Serial Number  Availability
-----
cluster1               1-80-123456           Available
```

4. Delete each cluster peer relationship by using the `cluster peer delete` command from the source node to remove the configuration information and Snapshot copies from the source volume.

You must delete the cluster peer relationships from both clusters in the relationship.

Example

Assuming that cluster 1 and cluster 2 are in a cluster peer relationship, you delete the cluster peer relationship by using the following two commands:

```
cluster1::> cluster peer delete -cluster cluster2
cluster2::> cluster peer delete -cluster cluster1
```

SMB 3.0 must be disabled before reverting to a release earlier than Data ONTAP 8.2

Data ONTAP 8.2 and later releases provide support for SMB 3.0. Before you revert to a release earlier than Data ONTAP 8.2, you must disable SMB 3.0 on all Storage Virtual Machines (SVMs) in the cluster.

- The following advanced-level command disables this feature on all SVMs:

```
vserver cifs options modify -vserver * -smb3-enabled false
```

- You need to be aware that several new features and functionality in Data ONTAP 8.2 and later releases are dependent on SMB 3.0, including the following:
 - Continuously available share property
 - Persistent handles
 - Remote VSS for SMB shares
 - Witness
 - ODX copy offload
 - BranchCache version 2

Note: The Hyper-V over SMB solution depends on the functionality provided by the continuously available share property, persistent handles, Remote VSS for SMB shares, and the Witness protocol. You should not disable SMB 3.0 until you have taken appropriate actions for any Hyper-V over SMB solutions on the cluster. Before disabling SMB 3.0, ensure that there are no ongoing Remote VSS shadow copy operations.

For more information, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.

IPv6 configurations for CIFS must be reconfigured before reverting

Data ONTAP 8.2 and later releases provide support for IPv6 for CIFS. Before you revert to a release earlier than Data ONTAP 8.2, any configuration with only IPv6 addresses must be reconfigured with an IPv4 address.

This includes, but is not limited to the following:

- Storage Virtual Machine (SVM) data LIFs, routing groups, and static routes for SVMs hosting CIFS servers
- Preferred domain controllers

Note: Domain controllers and other servers providing services to CIFS servers must have IPv4 addresses configured to allow network connectivity after a revert to a version of Data ONTAP that does not support IPv6 for CIFS.

For more information about managing CIFS server configurations, see the *Clustered Data ONTAP File Access Management Guide for CIFS*. For more information about configuring IPv4 and IPv6, see the *Clustered Data ONTAP Network Management Guide*.

Actions you must take for FPolicy configurations before reverting to a release earlier than Data ONTAP 8.2

Data ONTAP 8.2 and later releases provide support for the FPolicy feature. Before you revert to a release earlier than Data ONTAP 8.2, you must understand and act on some important revert considerations.

Before reverting to a version of Data ONTAP that does not support FPolicy, the following conditions must be met:

- Every file on which FPolicy servers set the offline bit must be either deleted or replaced with the original files before disabling FPolicy and reverting to a version of Data ONTAP that does not support FPolicy.

Note: If you do not replace the files with the offline bit set with the original files prior to reverting, clients access the stub files instead of the files to which the stub refers.

- FPolicy functionality must be disabled on the cluster by disabling every FPolicy policy on the cluster.

For more information about managing FPolicy configurations, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.

Actions you must take for Hyper-V over SMB solutions before reverting to a release earlier than Data ONTAP 8.2

Data ONTAP 8.2 and later releases provide support for the Hyper-V over SMB solution. Before you revert to a release earlier than Data ONTAP 8.2, you must understand and act on some important revert considerations.

You must consider the following and take action where necessary:

- There must be no file access by the Hyper-V servers to virtual machine files when you revert:
 - You can use the Hyper-V application to migrate virtual machine files to another storage device or to local storage.
 - You can power down all virtual machines and manually terminate Hyper-V server connections to the data LIFs.

Data ONTAP disables SMB 3.0 before reverting; therefore, if the SMB connections are not manually terminated, Data ONTAP terminates them during the revert.

- You cannot use the Hyper-V over SMB solution if you revert to a version of Data ONTAP that does not support it.

If you want to store virtual machine files on Storage Virtual Machine (SVM) volumes, you must configure the Hyper-V servers to use connected LUNs to store and access virtual machine files. You must then copy the virtual machine files from the SMB shares to the connected LUNs.

- To revert, there can be no ongoing Remote VSS shadow copy operations.

If there are any, you must wait for the operations to finish or manually abort them before proceeding with the revert. If you need to abort any shadow copy operations, contact technical support for assistance. Upon a revert, Data ONTAP does not delete existing Snapshot copies.

- You must disable the Shadow Copy feature on all SVMs before reverting.

The following advanced privilege command disables this feature on all SVMs:

```
vserver cifs options modify -vserver * -shadowcopy-enabled false
```

- You must disable SMB 3.0 on all SVMs before reverting.

The following advanced privilege command disables this feature on all SVMs:

```
vserver cifs options modify -vserver * -smb3-enabled false
```

Note: Other CIFS functionality available on Data ONTAP 8.2 and later depends on SMB 3.0. You should not disable SMB 3.0 until you have taken appropriate action for other features and

functionality that depends on SMB 3.0. This includes the continuously available share property, persistent handles, Remote VSS for SMB shares, the Witness protocol, ODX copy offload, the CIFS reparse point option, and BranchCache 2.

For more information about managing the Hyper-V over SMB solution, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.

Actions you must take for local user and group configurations before reverting to a release earlier than Data ONTAP 8.2

Data ONTAP 8.2 and later releases provide support for local users and groups for CIFS servers. Before you revert to a release earlier than Data ONTAP 8.2, you must understand and act on some important revert considerations.

Before reverting to a version of Data ONTAP that does not support local users and groups for CIFS servers, you must consider the following and perform any applicable actions:

- Upon a revert to a prior major version of Data ONTAP, Data ONTAP does not use local users and groups during authentication and access token creation.
If there are users who authenticate by using local user accounts and they need continued access after revert, you must configure domain accounts that those users can use to authenticate.
- Local users and groups are not removed from file and folder ACLs.
File access requests that depend on access being granted because of permissions granted to local users or groups are denied. To allow access, you must reconfigure file permissions to allow access based on domain users and groups instead of local users and groups.
- You must disable the local users and groups feature on all Storage Virtual Machines (SVMs) before reverting.

The following advanced privilege command disables this feature on all SVMs:

```
vserver cifs options modify -vserver * -is-local-users-and-groups-enabled false
```

For more information about managing local users and groups and managing SMB access, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.

Export policies must be configured for SMB access before reverting

Before you revert to a release earlier than Data ONTAP 8.2, you must configure export policies for SMB access on Storage Virtual Machines (SVMs) where data is accessed over SMB shares.

For releases earlier than Data ONTAP 8.2, export policies are mandatory for SMB access. Starting with Data ONTAP 8.2, export policies for SMB access are optional and are disabled by default. If you revert to a version of Data ONTAP where export policies are mandatory, export policies are turned on and required for SMB access. If you do not have export policies in place that permit SMB access prior to reverting, SMB clients are denied access to data over SMB shares.

The recommendation is that you configure export policies for SMB on all SVMs with SMB shares before you revert so that there are not hard-to-resolve SMB client access issues after the revert is complete.

For more information about configuring export policies for SMB access, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.

BranchCache must be disabled before reverting to a release earlier than Data ONTAP 8.2

Data ONTAP 8.2 and later releases provide support for BranchCache. Before you revert to a release earlier than Data ONTAP 8.2, you must disable BranchCache on all Storage Virtual Machines (SVMs) in the cluster.

- The following command disables this feature on all SVMs:

```
vserver cifs branchcache delete -vserver * -flush-hashes true
```

This command deletes the BranchCache configuration and hashes on all SVMs. After the revert is complete, the storage administrator can manually delete the directories that contained hash stores, if desired.

- When you revert to a version of Data ONTAP that does not support BranchCache, the SMB shares do not advertise BranchCache capabilities to BranchCache-enabled clients; therefore, the clients do not request hash information.

Instead, they request the actual content using normal SMB read requests.

For more information about managing BranchCache configurations, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.

Reverting systems with deduplicated volumes

Before reverting from the Data ONTAP 8.2 release family, you must ensure that the volumes contain sufficient free space for the revert operation.

About this task

Reverting from a Data ONTAP 8.2 release family on a system that has deduplication enabled, includes running advanced mode commands. You must contact technical support for assistance.

If you have enabled both deduplication and data compression on a volume that you want to revert, then you must revert data compression before reverting deduplication.

Steps

1. Use the `volume efficiency show` command with the `-fields` option to view the progress of efficiency operations running on the volumes.

Example

The following command displays the progress of efficiency operations:

```
volume efficiency show -fields vserver,volume,progress
```

2. Use the `volume efficiency stop` command with the `-all` option to stop all active and queued deduplication operations.

Example

The following command stops all active and queued deduplication operations on volume VolA:

```
volume efficiency stop -vserver vs1 -volume VolA -all
```

3. Use the `volume efficiency off` command to disable the deduplication operation.

Example

The following command disables deduplication operation on volume VolA:

```
volume efficiency off -vserver vs1 -volume VolA
```

4. Use the `set -privilege advanced` command to log in at the advanced privilege level.
5. Use the `volume efficiency revert-to` command with the `-version` option to downgrade the efficiency metadata of a volume to a specific version of Data ONTAP.

Example

The following command reverts the efficiency metadata on volume VolA to 8.1 version:

```
volume efficiency revert-to -vserver vs1 -volume VolA -version 8.1
```

Note: The `volume efficiency revert-to` command reverts volumes that are present on the node on which this command is executed. This command does not revert volumes across nodes.

6. After the revert operation is complete, return to the admin privilege level by entering the following command:

```
set -privilege admin
```

For more information about deduplication, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Reverting systems with compressed volumes

Before reverting from the Data ONTAP 8.2 release family, you must ensure that the volumes contain sufficient free space for the revert operation.

Before you begin

If you are reverting from Data ONTAP 8.2 release family, then you must have deleted all the Snapshot copies that have compressed data and decompress the data in the volumes.

About this task

Reverting from a Data ONTAP 8.2 release on a system that has data compression enabled, includes running advanced mode commands. You must contact technical support for assistance.

Steps

1. Use the `volume efficiency show` command with the `-fields` option to view the progress of efficiency operations running on the volumes.

Example

The following command displays the progress of efficiency operations:

```
volume efficiency show -fields vsserver,volume,progress
```

2. Use the `volume efficiency stop` command with the `-all` option to stop all active and queued data compression operations on the volume.

Example

The following command aborts both active and queued data compression operations on volume VolA:

```
volume efficiency stop -vsserver vs1 -volume VolA -all
```

3. Use the `volume efficiency modify` command to disable data compression on the volume.

Example

The following command disables data compression on volume VolA:

```
volume efficiency modify -vsserver vs1 -volume VolA -compression false -inline-compression false
```

4. Use the `volume efficiency off` command to disable deduplication on the volume.

Example

The following command disables deduplication on volume VolA:

```
volume efficiency off -vsserver vs1 -volume VolA
```

5. Use the `set -privilege advanced` command to log in at the advanced privilege level.
6. Use the `volume efficiency revert-to` command with the `-version` option to downgrade the efficiency metadata of a volume a Data ONTAP 8.1 release family.

Example

If you are reverting to Data ONTAP 8.1 release, the following command downgrades the efficiency metadata on volume VolA to 8.1 version:

```
volume efficiency revert-to -vsserver vs1 -volume VolA -version 8.1
```

Note: The `volume efficiency revert-to` command reverts volumes that are present on the node on which this command is executed. This command does not revert volumes across nodes.

7. After the revert operation is complete, use the `set -privilege admin` command to return to the admin privilege.

For more information about data compression, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Deleting an SVM with Infinite Volume

If the cluster contains an Infinite Volume, you must delete the Infinite Volume and its containing Storage Virtual Machine (SVM) before reverting or downgrading from Data ONTAP 8.1.1 or a later release of the Data ONTAP 8.1 family to the first release in the Data ONTAP 8.1 family.

Before you begin

- The Infinite Volume must be unmounted.
- Any SnapMirror relationships with the Infinite Volume must be deleted.

Steps

1. If the Infinite Volume is online, use the `volume offline` command to take the Infinite Volume offline.
2. Use the `volume delete` command to delete the Infinite Volume.
3. Use the `volume delete` command to delete any FlexVol volumes that were created for data protection or recovery purposes.
4. Delete any customized user accounts and roles associated with the SVM.

For information about users and roles, see the *Clustered Data ONTAP File Access Management Guide for CIFS* and the *Clustered Data ONTAP File Access Management Guide for NFS*.

5. Use the `vserver stop` command to stop the SVM.
6. Use the `vserver delete` command to delete the SVM.
7. Reboot all the nodes in the cluster.

Verifying the system time

You should verify that NTP is configured, and that the time is synchronized across the cluster.

About this task

For more information about managing the system time, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

1. Use the `system services ntp server show` command to verify that each node is associated with an NTP server.

Example

```
cluster1::> system services ntp server show
Node   Server                      Version
-----
node0
      ntp1.example.com        max
      ntp2.example.com        max
node1
      ntp1.example.com        max
      ntp2.example.com        max
node2
      ntp1.example.com        max
      ntp2.example.com        max
node3
      ntp1.example.com        max
      ntp2.example.com        max
```

2. Verify that each node has the same date and time:

If you are running Data ONTAP...	Enter the following command...
8.1.x	system node date show
8.2.x	cluster date show

Example

```
cluster1::> cluster date show
Node   Date                      Timezone
-----
node0   4/6/2013 20:54:38         GMT
node1   4/6/2013 20:54:38         GMT
node2   4/6/2013 20:54:38         GMT
node3   4/6/2013 20:54:38         GMT
4 entries were displayed.
```

Preparing Snapshot copies before reverting

Before reverting to an earlier Data ONTAP release, you must delete any Snapshot copies that were created after upgrading to the current release, delete root aggregate and root volume Snapshot copies, and disable Snapshot schedules for the root aggregate and root volume.

Before you begin

If you are reverting in a SnapMirror environment, you must first have deleted the following mirror relationships:

- All load-sharing mirror relationships
- Any data protection mirror relationships that were created in Data ONTAP 8.2.x
- All data protection mirror relationships if the cluster was re-created in Data ONTAP 8.2.x

FlexClone volumes that contain Snapshot copies that were created in Data ONTAP 8.2 or later must be either split from their parents or deleted. You will not be able to delete the Snapshot copies until these FlexClone volumes are split or deleted.

About this task

Root aggregate and root volume Snapshot copies are not visible from the clustershell and are not deleted by a `snapshot delete` command; therefore, you must delete the Snapshot copies manually.

Steps

1. Identify any Snapshot copies that were created after upgrading to the current release:

```
volume snapshot show -fs-version 8.2
```

2. Delete the Snapshot copies that you identified:

```
volume snapshot delete {-fs-version 8.2 -node nodename}
```

3. Identify the root aggregate on each node in the cluster by using the `run -node nodename aggr status` command.

You identify the root aggregate by the word `root` in the options column of the `aggr status` command output.

Example

```
cluster1::> run -node node1 aggr status
```

Aggr	State	Status	Options
aggr0	online	raid_dp, aggr 64-bit	root

4. Disable Snapshot schedules on the root aggregate:

```
run -node nodename aggr options root_aggr_name nosnap on
```

5. Delete the root aggregate Snapshot copies:

```
run -node nodename snap delete -A -a -f aggr_name
```

6. Identify the root volume on each node in the cluster by using the `run -node nodename vol status` command.

You identify the root volume by the word `root` in the Options column of the `vol status` command output.

Example

```
vs1::> run -node node1 vol status
```


Volume	State	Status	Options
vol0	online	raid_dp, flex 64-bit	root, nvfail=on

7. Disable Snapshot schedules on the root volume:

```
run -node nodename vol options root_volume_name nosnap on
```

8. Delete the root volume Snapshot copies:

```
run -node nodename snap delete -a -f volume_name
```

Obtaining Data ONTAP software images

You must copy a software image from the NetApp Support Site to an HTTP or FTP server on your network so that nodes can access the images by using the `system node image update` command.

About this task

To upgrade, revert, or downgrade the cluster to the target release of Data ONTAP, you need access to software images. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site. Note the following important information:

- Software images are specific to platform models.
Be sure to obtain the correct image for your cluster.
- Software images include the latest version of system firmware that was available when a given version of Data ONTAP was released.

Steps

1. Locate the target Data ONTAP software in the **Software Downloads** area of the NetApp Support Site.
2. Copy the software image (for example, `821_q_image.tgz`) from the NetApp Support Site to the directory on the HTTP or FTP server from which the image will be served.

Related information

[Download Software: support.netapp.com/NOW/cgi-bin/software](https://support.netapp.com/NOW/cgi-bin/software)

Installing Data ONTAP software images in a cluster

If needed, install the target Data ONTAP 8.x image software package, but leave the default set to the current Data ONTAP 8.x version.

Before you begin

You must have obtained the Data ONTAP software images.

Steps

1. Choose one of the following options based on your requirements:

If you want to...	Enter this command...
Download, but not install, the software image	<pre>system node image get -node * -package location -replace-package true -background true</pre> <p>This command downloads the software image to all of the nodes simultaneously. To download the image to each node one at a time, do not specify the <code>-background</code> parameter.</p>
Install a previously downloaded software image	<pre>system node image update -node * -package file:///mroot/etc/software/image_name -background true</pre> <p>Note the following considerations for this command:</p> <ul style="list-style-type: none">• If you are currently running Data ONTAP 8.2, the <code>-package</code> parameter only requires you to enter the image name; you do not need to enter the full directory path.• If you are unsure of the image name to install, you can view a list of previously downloaded software images by using the <code>system node image package show</code> command.• This command installs the software image on all of the nodes simultaneously. To install the image on each node one at a time, do not specify the <code>-background</code> parameter.
Download and install the software image in the same operation	<pre>system node image update -node * -package location -replace-package true -background true</pre> <p>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 <code>-background</code> parameter.</p>

2. 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.

Example

This example shows a 2-node cluster in which the software image has been 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:   Installation complete. image2 updated on node node0.
There is no update/install in progress
Status of most recent operation:
Run Status:     Exited
Exit Status:    Success
Phase:         Run Script
Exit Message:   Installation complete. image2 updated on node node1.
2 entries were acted on.

```

Reverting a Data ONTAP cluster

To take the cluster offline to revert to an earlier Data ONTAP release, you must disable storage failover and the data LIFs, address reversion preconditions, revert the cluster and filesystem configurations on a node, and then repeat the process for each additional node in the cluster.

Before you begin

You must have satisfied reversion preparation requirements.

About this task

Reverting a cluster requires you to take the cluster offline for the duration of the reversion.

Steps

1. Verify that the target Data ONTAP software is installed:

```
system node image show
```

Example

This example shows that version 8.1.2 is installed as the alternate image on both nodes.

```

cluster1::> system node image show

```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	8.2.1	11/25/2013 12:37:36
	image2	false	false	8.1.2	4/22/2013 13:52:22
node1	image1	true	true	8.2.1	11/25/2013 12:41:16
	image2	false	false	8.1.2	4/22/2013 13:55:22

```

4 entries were displayed.

```

For more information about installing the target Data ONTAP software image, see [Installing Data ONTAP 8.x software images in a cluster](#).

2. Set the target Data ONTAP software image to be the default image:

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

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

```
system node image show
```

Example

This example shows that version 8.1.2 is set as the default image on both nodes.

```
cluster1::> system node image show
Node      Image      Is      Is      Version      Install
-----  -
node0     image1     false   true    8.2.1        11/25/2013 12:37:36
          image2     true    false   8.1.2        4/22/2013 13:52:22
node1     image1     false   true    8.2.1        11/25/2013 12:41:16
          image2     true    false   8.1.2        4/22/2013 13:55:22
4 entries were displayed.
```

4. Disable all of the data LIFs in the cluster:

```
network interface modify {-role data} -status-admin down
```

5. If the cluster consists of only two nodes, disable cluster HA:

```
cluster ha modify -configured false
```

6. Disable storage failover for the nodes in the HA pair by entering the following command for either node:

```
storage failover modify -node nodename -enabled false
```

You only need to disable storage failover once for the HA pair. When you disable storage failover for a node, storage failover is also disabled on the node's partner.

7. Set the privilege level to advanced:

```
set -privilege advanced
```

8. If the cluster consists of only two nodes, then verify that the node does not hold epsilon by doing the following:

- a. Check to see if the node currently holds epsilon:

```
cluster show -node nodename
```

Example

This example shows that the node holds epsilon.

```
cluster1::*> cluster show -node node1
Node: node1
UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
Epsilon: true
Eligibility: true
Health: true
```

- b. If the node holds epsilon, then mark epsilon false on the node so that epsilon can be transferred to the node's partner:

```
cluster modify -node nodenameA -epsilon false
```

- c. Transfer epsilon to the node's partner by marking epsilon true on the partner node:

```
cluster modify -node nodenameB -epsilon true
```

9. Verify that the node is ready for reversion:

```
system node revert-to -node nodename -check-only true -version 8.1
```

The `check-only` parameter identifies any preconditions that must be addressed before reverting, such as the following examples:

- Disabling storage failover
- Disabling the Snapshot policy
- Deleting Snapshot copies that were created after upgrading to the later release family

Proceed to the next step when all identified preconditions have been addressed.

10. Verify that all of the preconditions have been addressed:

```
system node revert-to -node nodename -check-only true -version 8.1
```

11. Revert the cluster configuration of the node:

```
system node revert-to -node nodename -version 8.1
```

The `-version` option refers to the target release family. For example, if the software you installed and verified in Step 2 is Data ONTAP 8.1.2, the correct value of the `-version` option is 8.1.

The cluster configuration is reverted, and then you are logged out of the clustershell.

12. Log back into the clustershell, and then switch to the nodeshell:

```
system node run -node nodename
```

13. Revert the filesystem configuration of the node:

```
revert_to 8.1c
```

This command verifies that the node's filesystem configuration is ready to be reverted and then reverts it. If any preconditions are identified, you must address them and then reenter the `revert_to` command.

When the command finishes, the LOADER prompt is displayed.

14. At the LOADER prompt, enter the following command to boot to the target release:

```
boot_ontap
```

15. Repeat Steps 8 on page 124 through 14 on page 125 on the other node in the HA pair.

16. If the cluster consists of only two nodes, reenabling cluster HA:

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

17. Reenable storage failover on both nodes if it was previously disabled:

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

18. Repeat Steps 6 on page 124 through 17 on page 125 for each additional HA pair in the cluster.

Completing post-reversion tasks

After reverting to an earlier Data ONTAP release family, you might need to perform additional tasks to ensure cluster health and storage availability.

You should also verify that any services that you halted manually restarted after the reversion. If not, you should restart those services manually and verify that any clients have appropriate access to cluster services.

Verifying that the cluster is in quorum

Before and after you perform an upgrade, reversion, or downgrade, you must ensure that all nodes are participating in a replicated database (RDB) quorum and that all rings are in the quorum. You must also verify that the per-ring quorum master is the same for all nodes.

About this task

For more information about cluster replication rings and RDB quorums, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

Enter **y** to continue.

2. Display each RDB process:

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 vldb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.1.x:

```
cluster1::*> cluster ring show -unitname vldb
Node    UnitName Epoch DB Epoch DB Trnxs Master
```

```

-----
node0  vldb      154   154      14847   node0
node1  vldb      154   154      14847   node0
node2  vldb      154   154      14847   node0
node3  vldb      154   154      14847   node0
4 entries were displayed.

```

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.2.x:

```

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.

```

For each process, verify the following configuration details:

- The relational database epoch and database epochs match for each node.
- The per-ring quorum master is the same for all nodes.
Note that each ring might have a different quorum master.

3. Return to the admin privilege level:

```
set -privilege admin
```

4. 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. During the upgrade, reversion, or downgrade process, each node will temporarily fall out of SAN quorum. Therefore, if you are verifying the SAN quorum after completing an upgrade, reversion, or downgrade, you may notice critical event messages warning you that the nodes were previously out of SAN quorum.

If a node is out of SAN quorum, you can use the `storage failover takeover` and `storage failover giveback` commands to perform a planned takeover and giveback with the node's high-availability partner and bring the node back into SAN quorum.

Example

In this example, both nodes in the cluster are in SAN quorum.

```

cluster1::> event log show -messagename scsiblade.*
Time      Node      Severity      Event
-----
8/13/2013 14:03:51 node0     INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 14:03:51 node1     INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...

```

Example

This example shows a two-node cluster after performing an upgrade. Each node shows a previous out of SAN quorum event message from when the node was upgraded. However, the most recent event message for each node shows that both nodes are presently in SAN quorum.

```
cluster1::> event log show -messagename scsiblade.*
Time           Node           Severity      Event
-----
8/13/2013 15:37:51 node1         INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:31:26 node1         CRITICAL       scsiblade.out.of.quorum: This node ...
8/13/2013 15:31:26 node1         INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:31:26 node1         INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:30:43 node0         INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:24:16 node0         CRITICAL       scsiblade.out.of.quorum: This node ...
8/13/2013 15:24:16 node0         INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:24:16 node0         INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
```

Verifying cluster and SVM health

Before and after you upgrade, revert, or downgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and the aggregates and volumes are online.

Steps

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster:

```
cluster show
```

Example

```
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. For more information about EMS messages, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

To troubleshoot cluster health issues, see the knowledgebase article [Troubleshooting Workflow: RDB app out of quorum](#) on the NetApp Support Site.

2. Determine if any disk drives are broken, undergoing maintenance, or reconstructing:

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

To check for...	Do this...
Disks undergoing maintenance or reconstructing	<p>a. Display any disks in maintenance, pending, or reconstructing states:</p> <pre>storage disk show -state maintenance pending reconstructing</pre> <p>b. Wait for the maintenance or reconstruction operation to complete before proceeding.</p>

3. To verify that all aggregates are online, display the state of physical and logical storage, including storage aggregates:

```
storage aggregate show -state !online
```

This command displays the aggregates that are *not* online.

Example

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

For more information about managing aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide*.

4. To verify that all volumes are online, display any volumes *not* online:

```
volume show -state !online
```

Example

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

For more information about managing volumes, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Enabling and reverting LIFs to home ports

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

About this task

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.

Steps

1. Display the status of all LIFs:

```
network interface show
```

Example

This example displays the status of all LIFs for a Storage Virtual Machine (SVM, formerly known as Vserver).

```
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
```

Example

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

3. Revert LIFs to their home ports:

```
network interface revert *
```

Example

This command reverts all LIFs back to their home ports and changes all LIF home statuses to true.

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

4. Verify that all LIFs are in their home ports:

```
network interface show
```

Example

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.

Preparing Snapshot copies after reverting

After reverting to an earlier version of Data ONTAP, you must enable Snapshot schedules of the root volume and root aggregate to start creating Snapshot copies again.

About this task

You are reenabling the Snapshot schedules of the root volume and root aggregate that you disabled before you reverted to an earlier version of Data ONTAP.

Steps

1. Enable the Snapshot schedule of the root volume by using the run `-node nodename vol options root_vol_name nosnap off` command.

Example

```
cluster1::> run -node node1 vol options vol0 nosnap off
```

2. Enable the Snapshot schedule of the root aggregate by using the run `-node nodename aggr options root_aggr_name nosnap off` command.

Example

```
cluster1::> run -node node1 aggr options aggr0 nosnap off
```

Verifying client access (CIFS and NFS)

For the configured protocols, test access from CIFS and NFS clients to verify that the cluster is accessible.

Considerations for downgrading the SP firmware

If your current SP firmware version is not supported for the Data ONTAP release you are downgrading or reverting to, you must install a supported SP firmware version for the earlier Data ONTAP release.

After the Data ONTAP revert or downgrade process is complete, you must take the action to install an SP firmware version that is supported for the Data ONTAP version you reverted or downgraded to. To learn which SP firmware versions are supported by each Data ONTAP release, see the [BIOS Service Processor Support Matrix](#) on the NetApp Support Site. For instructions about downloading and installing an SP firmware version, see the [System Firmware and Diagnostics Download](#) page on the NetApp Support Site.

Reinstalling the required V-Series license after revert or downgrade

The licensing scheme for V-Series systems changed in Data ONTAP 8.2. Data ONTAP 8.2 and later requires the V_StorageAttach license package for V-Series systems to be able to access LUNs on storage arrays. Depending on the type of reversion you do, you might need to install the v-series license key for a prior release.

A license key is required for each V-Series system being reverted or downgraded.

If...	Then the V-Series license requirement is...
The V-Series system was upgraded to Data ONTAP 8.2 from the 8.1.x release family and you want to revert to a release in the 8.1.x release family again	You do not have to install the V-Series license for the release to which the system is being reverted. Data ONTAP remembers the V-Series license from when it was upgraded from 8.1.x to 8.2; Data ONTAP reinstalls those licenses when Data ONTAP is downgraded to 8.1.x.
Data ONTAP 8.2 is the first release of Data ONTAP installed on the system and you want to revert to a release in the 8.1.x release family	You must manually install the license key for V-Series systems that is supported for the release to which the system is being reverted. Contact your sales representative to obtain the appropriate license key for your system and release.
You want to downgrade the system from Data ONTAP 8.2.x to an earlier release in the 8.2 release family	You do not have to install the V_StorageAttach license package; Data ONTAP remembers the appropriate license for the release family.

For information about how to install licenses, see the *Clustered Data ONTAP System Administration Guide for SVM Administrators*.

Enabling capability for SVM administrator with vsadmin role

After reverting to an earlier version of clustered Data ONTAP, the event generate-autosupport-log capability becomes unavailable for the predefined role vsadmin. Therefore, you must create a custom role with command directory name as `event generate autosupport log` and create a user for the new role.

About this task

With the new custom role, the SVM administrator can execute the `event generate-autosupport-log` command or `zapi` equivalent.

Steps

1. Use the `security login role create` command to create a new SVM administrator role.

Example

The following example shows how to create a new role test:

```
cluster1::>security login role create -role test -cmddirname "event
generate-autosupport-log" -access all -query "" -vserver vs1
```

2. Use the `security login create -username` command to create a new user and assign new role to the user.

Example

The following example shows how to create a new user and assign the new role:

```
cluster1::>security login create -username user_test1 -application
ontapi -authmethod password -role test -vserver vs1
```

Downgrading clusters to an earlier release in the same release family

Transitioning a cluster to an earlier release in the same Data ONTAP release family is referred to as a *downgrade*. Doing so requires preparation, downloading and booting the earlier release, and completing post-downgrade procedures.

Downgrading does not require modifications to Data ONTAP on-disk structures; you must simply obtain and boot the target release after verifying requirements and compatibility.

When to downgrade and when to call technical support

You can downgrade without assistance when downgrading new or test clusters, but you should call technical support if you encounter problems during or after upgrading, or if you want to downgrade a production cluster.

You can downgrade to an earlier release family without assistance from technical support only in the following scenarios:

- You upgraded to a new release on a test cluster and you want to return to the original release when testing is completed.
- You are configuring a new cluster—running a later release of Data ONTAP and not yet in production—in an environment in which you have standardized on an earlier Data ONTAP release.

Do not attempt to downgrade Data ONTAP in a production environment without assistance. If you encounter any of the following circumstances, contact technical support immediately:

- The upgrade process fails and cannot finish.
- The upgrade process finishes, but the cluster is unusable in a production environment.
- The upgrade process finishes and the cluster goes into production, but you are not satisfied with its behavior.
- The upgrade process finishes for some but not all of the nodes, and you decide that you want to downgrade.

Planning your downgrade

Because new features are introduced in each release of Data ONTAP, you must understand downgrade requirements and evaluate how they might impact your current configuration.

Before proceeding with the downgrade, you should plan to do the following:

- Review the *Release Notes* for the Data ONTAP downgrade source release.

- Understand any requirements for downgrading to the target release from your existing software.
- Note any potential functionality changes to your cluster after the downgrade.
- Be prepared to address all points in the downgrade checklist.

Cluster downgrade checklist

You can use this checklist to record your progress as you prepare for the downgrade, perform the downgrade, and complete post-downgrade tasks.

Steps for preparing to downgrade

Preparatory steps are complete when all of the following conditions are true:

Condition	Complete?
Software and hardware support in the target release is confirmed. To confirm hardware support, visit <i>Hardware Universe</i> at hwu.netapp.com	
All release-specific downgrade issues have been resolved.	
You have clustershell access privileges.	
The cluster and Storage Virtual Machines (SVMs) are running and healthy. All aggregates and volumes should be healthy and online before proceeding with the reversion. You can use the <code>cluster show</code> command to verify the status of the nodes.	
The cluster is in quorum. All nodes are participating in a quorum and all rings are in the quorum. The per-ring quorum master should be the same for all nodes.	
LIFs are online and on their correct home ports. You can use the <code>network interface</code> command to display and modify LIF configuration.	
The system time is synchronized across the cluster.	
If you are preparing to downgrade a storage system with array LUNs, no back-end configuration errors exist. You can check for back-end configuration errors using the <code>storage array config show</code> command.	
Any CIFS sessions that are not continuously available have been terminated.	

Condition	Complete?
Each node is running Data ONTAP 8.2.0 or later. Ensure that you are running on the minimum software version allowed for the downgrade by running the <code>system node image show</code> command.	
You have the target Data ONTAP software image available on an HTTP or FTP server. Download the software image for the target Data ONTAP release from the NetApp Support Site at support.netapp.com , and place it on an HTTP or FTP server that is accessible by each node.	
The target Data ONTAP software images are installed on each node and set as the alternate boot device image. You can use the <code>system node image update</code> command to install the software images. You can use the <code>system node image show</code> command to verify that the software images are installed as the alternate boot image on each node.	
SnapMirror operations are suspended.	

Steps for performing a nondisruptive downgrade

The nondisruptive downgrade is complete when all of the following steps have been completed:

Condition	Complete?
No jobs are running. If any aggregate, volume, mirror, NDMP (dump or restore), or Snapshot jobs are running or queued, allow the jobs to complete successfully or stop the queued entries.	
The target Data ONTAP software is installed and set as the default boot image.	
Each HA pair is downgraded.	<div>The first node in the HA pair is downgraded.</div> <div>The node's partner is downgraded.</div>

Steps for performing a disruptive downgrade

Condition	Complete?
No jobs are running. If any aggregate, volume, mirror, NDMP (dump or restore), or Snapshot jobs are running or queued, allow the jobs to complete successfully or stop the queued entries.	
The target Data ONTAP software is installed and set as the default boot image.	
Each node is rebooted.	

Steps for after downgrading

Post-downgrade steps are complete when all of the following conditions are true:

Condition	Complete?
The cluster is in quorum. Ensure that all nodes are participating in a quorum and all rings are in the quorum. Verify also that the per-ring quorum master is the same for all nodes.	
The cluster and SVMs are running and healthy. All aggregates and volumes should be healthy and online after the reversion. You can use the <code>cluster show</code> command to verify the status of the nodes.	
LIFs are online and on their correct home ports. You can use the <code>network interface</code> command to display and modify LIF configuration.	
Client access is verified. You should verify that clients can access the cluster for each configured protocol.	
SnapMirror operations are resumed.	
The Service Processor firmware version is confirmed. If your current SP firmware version is not supported for the Data ONTAP release to which you reverted, you must install a supported SP firmware version for the earlier Data ONTAP release.	

What to check before downgrading V-Series systems

The process of downgrading systems with native disks is the same for V-Series systems and FAS systems. V-Series systems that use array LUNs require some special checks in addition to the checks for all systems running Data ONTAP.

Before downgrading a system running Data ONTAP 8.2 that uses array LUNs, check for the following:

- Whether you are using functionality that is supported in Data ONTAP 8.2 but not in the release to which you are downgrading your system
- Whether there are back-end storage related configuration errors

Storage Encryption downgrade restriction

If your storage system is configured for Storage Encryption, do not attempt to install and run any Data ONTAP version earlier than 8.2.1. Doing so would disable your system and render your data inaccessible.

Downgrade process considerations

Make sure that you know about downgrade issues and limitations before downgrading clusters to an earlier version of Data ONTAP.

Be aware of the following issues:

- After you upgrade clusters to Data ONTAP 8.2, you can downgrade to an earlier release in the Data ONTAP 8.2 release family.
For example, you can downgrade from Data ONTAP 8.2.1 to 8.2.0.
- Downgrading affects all nodes in the cluster.
The downgrade must be performed on all nodes in the cluster; however, some of the procedures must be performed on each HA pair and completed on each set of nodes before other pairs are downgraded.
- You can downgrade Data ONTAP nondisruptively.
During the downgrade process, the cluster remains online and continues to serve data.
- If your cluster serves CIFS clients, nondisruptive downgrades are supported for Hyper-V over SMB solutions.
Hyper-V over SMB solutions enable Hyper-V and the contained virtual machines to remain online and to provide continuous availability during the Data ONTAP downgrade. For more information, see the *Clustered Data ONTAP File Access Management Guide for CIFS*.
For all other CIFS configurations, client sessions are terminated. You should direct users to end their sessions before you downgrade to prevent data loss.
- Data ONTAP clusters can operate for a limited time in a *mixed version* state, in which nodes in a cluster are running Data ONTAP versions from different release families. However, the upgrade is not complete until all nodes are running the new target release.

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

Identifying downgrade issues

Every Data ONTAP release family has unique downgrade requirements that you must understand and resolve before you decide to downgrade.

For additional information, and to check for downgrade issues that might have been discovered later, see the *Clustered Data ONTAP Release Notes*. The following list summarizes downgrade issues known when this guide was published:

- If your current SP firmware version is not supported for the Data ONTAP release that you are downgrading or reverting to, you must install a supported SP firmware version for the earlier Data ONTAP release.
- If you downgrade or revert to a release earlier than Data ONTAP 8.2.1, you must run the `security ssh prepare-to-downgrade` command at the advanced privilege level to reset the SSH security configurations of the cluster and all Storage Virtual Machines (SVMs) to the default settings used in the earlier release.
- Exporting qtrees is not supported in releases earlier than Data ONTAP 8.2.1.
If you plan to downgrade or revert to an earlier release, you must first take certain actions; otherwise, the downgrade or revert operation fails.

Preparing for the Data ONTAP downgrade process

Before downgrading, you need to verify cluster health, verify aggregate and volume health, and install the target Data ONTAP image.

Verifying that the cluster is in quorum

Before and after you perform an upgrade, reversion, or downgrade, you must ensure that all nodes are participating in a replicated database (RDB) quorum and that all rings are in the quorum. You must also verify that the per-ring quorum master is the same for all nodes.

About this task

For more information about cluster replication rings and RDB quorums, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

Enter **y** to continue.

2. Display each RDB process:

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 vldb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.1.x:

```
cluster1::*> cluster ring show -unitname vldb
Node    UnitName Epoch DB Epoch DB Trnxs Master
-----
node0   vldb      154   154      14847  node0
node1   vldb      154   154      14847  node0
node2   vldb      154   154      14847  node0
node3   vldb      154   154      14847  node0
4 entries were displayed.
```

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.2.x:

```
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.
```

For each process, verify the following configuration details:

- The relational database epoch and database epochs match for each node.
 - The per-ring quorum master is the same for all nodes.
- Note that each ring might have a different quorum master.

3. Return to the admin privilege level:

```
set -privilege admin
```

4. 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. During the upgrade, reversion, or downgrade process, each node will temporarily fall out of SAN quorum. Therefore, if you are verifying the SAN quorum after completing an upgrade, reversion, or downgrade, you may notice critical event messages warning you that the nodes were previously out of SAN quorum.

If a node is out of SAN quorum, you can use the `storage failover takeover` and `storage failover giveback` commands to perform a planned takeover and giveback with the node's high-availability partner and bring the node back into SAN quorum.

Example

In this example, both nodes in the cluster are in SAN quorum.

```
cluster1:> event log show -messagename scsiblade.*
Time           Node           Severity      Event
-----
8/13/2013 14:03:51 node0          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 14:03:51 node1          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
```

Example

This example shows a two-node cluster after performing an upgrade. Each node shows a previous out of SAN quorum event message from when the node was upgraded. However, the most recent event message for each node shows that both nodes are presently in SAN quorum.

```
cluster1:> event log show -messagename scsiblade.*
Time           Node           Severity      Event
-----
8/13/2013 15:37:51 node1          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:31:26 node1          CRITICAL      scsiblade.out.of.quorum: This node ...
8/13/2013 15:31:26 node1          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:31:26 node1          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:30:43 node0          INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:24:16 node0          CRITICAL      scsiblade.out.of.quorum: This node ...
8/13/2013 15:24:16 node0          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:24:16 node0          INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
```

Verifying cluster and SVM health

Before and after you upgrade, revert, or downgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and the aggregates and volumes are online.

Steps

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster:

```
cluster show
```

Example

```
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. For more information about EMS messages, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

To troubleshoot cluster health issues, see the knowledgebase article [Troubleshooting Workflow: RDB app out of quorum](#) on the NetApp Support Site.

2. Determine if any disk drives are broken, undergoing maintenance, or reconstructing:

To check for...	Do this...
Broken disks	<p>a. Display any broken disks:</p> <pre>storage disk show -state broken</pre> <p>b. Remove or replace any broken disks.</p>
Disks undergoing maintenance or reconstructing	<p>a. Display any disks in maintenance, pending, or reconstructing states:</p> <pre>storage disk show -state maintenance pending reconstructing</pre> <p>b. Wait for the maintenance or reconstruction operation to complete before proceeding.</p>

3. To verify that all aggregates are online, display the state of physical and logical storage, including storage aggregates:

```
storage aggregate show -state !online
```

This command displays the aggregates that are *not* online.

Example

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

For more information about managing aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide*.

4. To verify that all volumes are online, display any volumes *not* online:

```
volume show -state !online
```

Example

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

For more information about managing volumes, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Enabling and reverting LIFs to home ports

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

About this task

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.

Steps

1. Display the status of all LIFs:

```
network interface show
```

Example

This example displays the status of all LIFs for a Storage Virtual Machine (SVM, formerly known as Vserver).

```
cluster1::> network interface show -vservers 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
```

Example

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

3. Revert LIFs to their home ports:

```
network interface revert *
```

Example

This command reverts all LIFs back to their home ports and changes all LIF home statuses to true.

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

4. Verify that all LIFs are in their home ports:

network interface show

Example

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.

Identifying active CIFS sessions that should be terminated

Before performing a minor nondisruptive upgrade or downgrade within the Data ONTAP 8.2 release family, you should identify and gracefully terminate any CIFS sessions that are not continuously available.

About this task

Continuously available CIFS shares, which are accessed by Hyper-V clients using the SMB3 protocol, do not need to be terminated before upgrading or downgrading.

Steps

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.

Example

```
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: CIFS\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.

```

Each of the sessions identified by this command should be terminated before proceeding with the Data ONTAP upgrade or downgrade.

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*

Example

```

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.

```

Verifying the system time

You should verify that NTP is configured, and that the time is synchronized across the cluster.

About this task

For more information about managing the system time, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

- 1. Use the `system services ntp server show` command to verify that each node is associated with an NTP server.

Example

```
cluster1::> system services ntp server show
Node      Server                      Version
-----
node0
    ntp1.example.com          max
    ntp2.example.com          max
node1
    ntp1.example.com          max
    ntp2.example.com          max
node2
    ntp1.example.com          max
    ntp2.example.com          max
node3
    ntp1.example.com          max
    ntp2.example.com          max
```

- 2. Verify that each node has the same date and time:

If you are running Data ONTAP...	Enter the following command...
8.1.x	<code>system node date show</code>
8.2.x	<code>cluster date show</code>

Example

```
cluster1::> cluster date show
Node      Date                      Timezone
-----
node0     4/6/2013 20:54:38          GMT
node1     4/6/2013 20:54:38          GMT
node2     4/6/2013 20:54:38          GMT
node3     4/6/2013 20:54:38          GMT
4 entries were displayed.
```

Checking for back-end configuration errors

Before downgrading V-Series systems to an earlier release, you need to run `storage errors show` to determine whether there are any back-end configuration errors.

Steps

- 1. Enter the following command:

storage array config show

2. Proceed based on the result of Step 1, as follows:

If...	Then...
If the <code>storage array config show</code> output <i>does not</i> instruct you to run <code>storage errors show</code>	Proceed with downgrading.
If the <code>storage array config show</code> output <i>does</i> instruct you to run <code>storage errors show</code>	Continue to the next step.

You are instructed to run the `storage errors show` command if Data ONTAP detects a back-end configuration error that would prevent Data ONTAP and the back-end storage array from operating together properly.

3. Enter the following command:

storage errors show

The `storage errors show` command provides details, at the array LUN level, as the following example shows:

Example

```
IBM_1742_1
-----
NAME (Serial #):  This Array LUN is only available on one path.
Proper configuration requires two paths.
```

4. Fix the problem indicated by `storage errors show`, then downgrade your system.

The *FlexArray Virtualization Installation Requirements and Reference Guide* contains explanations about errors shown in `storage errors show` output and provides information about how to fix them.

Determining the current software version on each node before downgrading

Ensure that you are running on the minimum software version allowed for the downgrade process by running the `system node image show` command.

Step

1. Determine the current software version:

system node image show

Example

```
cluster1::> system node image show
Node      Image      Is      Is      Version      Install
-----  -
node0     image1     true    true    8.2.1        11/27/2013 13:52:22
          image2     false   false   8.2.0        3/25/2013 12:37:36
node1     image1     true    true    8.2.1        11/27/2013 13:55:22
          image2     false   false   8.2.0        3/25/2013 12:41:16
4 entries were displayed.
```

Obtaining Data ONTAP software images

You must copy a software image from the NetApp Support Site to an HTTP or FTP server on your network so that nodes can access the images by using the `system node image update` command.

About this task

To upgrade, revert, or downgrade the cluster to the target release of Data ONTAP, you need access to software images. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site. Note the following important information:

- Software images are specific to platform models.
Be sure to obtain the correct image for your cluster.
- Software images include the latest version of system firmware that was available when a given version of Data ONTAP was released.

Steps

1. Locate the target Data ONTAP software in the **Software Downloads** area of the NetApp Support Site.
2. Copy the software image (for example, `821_q_image.tgz`) from the NetApp Support Site to the directory on the HTTP or FTP server from which the image will be served.

Related information

[Download Software: support.netapp.com/NOW/cgi-bin/software](http://support.netapp.com/NOW/cgi-bin/software)

Installing Data ONTAP software images in a cluster

If needed, install the target Data ONTAP 8.x image software package, but leave the default set to the current Data ONTAP 8.x version.

Before you begin

You must have obtained the Data ONTAP software images.

Steps

1. Choose one of the following options based on your requirements:

If you want to...	Enter this command...
Download, but not install, the software image	<pre>system node image get -node * -package location - replace-package true -background true</pre> <p>This command downloads the software image to all of the nodes simultaneously. To download the image to each node one at a time, do not specify the <code>-background</code> parameter.</p>
Install a previously downloaded software image	<pre>system node image update -node * -package file:/// mroot/etc/software/image_name -background true</pre> <p>Note the following considerations for this command:</p> <ul style="list-style-type: none">• If you are currently running Data ONTAP 8.2, the <code>-package</code> parameter only requires you to enter the image name; you do not need to enter the full directory path.• If you are unsure of the image name to install, you can view a list of previously downloaded software images by using the <code>system node image package show</code> command.• This command installs the software image on all of the nodes simultaneously. To install the image on each node one at a time, do not specify the <code>-background</code> parameter.
Download and install the software image in the same operation	<pre>system node image update -node * -package location - replace-package true -background true</pre> <p>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 <code>-background</code> parameter.</p>

2. 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.

Example

This example shows a 2-node cluster in which the software image has been 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:   Installation complete. image2 updated on node node0.
There is no update/install in progress
Status of most recent operation:
Run Status:     Exited
Exit Status:    Success
Phase:          Run Script
Exit Message:   Installation complete. image2 updated on node node1.
2 entries were acted on.

```

Preparing SnapMirror relationships for a nondisruptive upgrade or downgrade

You must suspend SnapMirror operations before performing a nondisruptive upgrade or downgrade of Data ONTAP.

About this task

For more information about SnapMirror operations, see the SnapMirror man pages and the *Clustered Data ONTAP Data Protection Guide*.

Steps

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.

Example

If you are upgrading from Data ONTAP 8.1, this example quiesces transfers involving the destination volume `vol1` from Storage Virtual Machine (SVM) `vs0` and cluster `cluster1`:

```
cluster1:> snapmirror quiesce -destination-path cluster1://vs0/vol1
```

Example

If you are downgrading within the Data ONTAP 8.2 release family, this example quiesces transfers involving the destination volume `vol1` from SVM `vs0`:

```
cluster1:> snapmirror quiesce -destination-path vs0:vol1
```

3. Verify that all SnapMirror relationships are quiesced:
snapmirror show -status !Quiesced

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

Example

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 transferring, do one of the following options:

Option	Description
Wait for the transfers to complete before performing the Data ONTAP upgrade.	Once each transfer completes, the relationship changes to <i>Quiesced</i> status.
Stop the transfers by entering the following command: snapmirror abort -destination-path destination -h	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 <i>Quiesced</i> status.
Note: You must use the <code>-foreground true</code> parameter if you are aborting load-sharing mirror transfers.	

Ensuring that no jobs are running

You must verify the status of cluster jobs before upgrading or downgrading to a different Data ONTAP release. 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, allow the jobs to finish successfully or stop the queued entries.

Steps

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

```
job show
```

Example

```
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			
8632	CLUSTER BACKUP AUTO daily	cluster1	-	Queued
	Description: Cluster Backup Job			
8633	CLUSTER BACKUP AUTO weekly	cluster1	-	Queued
	Description: Cluster Backup Job			

9944	SnapMirrorDaemon_7_2147484678	cluster1	node1	Dormant
	Description: Snapmirror Daemon for 7_2147484678			
18277	CLUSTER BACKUP AUTO 8hour	cluster1	-	Queued
	Description: Cluster Backup Job			
18377	SnapMirror Service Job	cluster1	node0	Dormant
	Description: SnapMirror Service Job			
18379	Network Consistency Diagnostic - weekly	cluster1	node0	Queued
	Description: Network Consistency Checker			
18385	Network Consistency Diagnostic - weekly	cluster1	node1	Queued
	Description: Network Consistency Checker			
9 entries were displayed				

2. Delete any running or queued aggregate, volume, or Snapshot copy jobs:

```
job delete -id job_id
```

Example

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

3. Ensure that no aggregate, volume, or Snapshot jobs are running or queued:

```
job show
```

Example

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

Performing the Data ONTAP downgrade process

To downgrade a cluster to an earlier Data ONTAP release in the same release family, you must install target images, address downgrade issues, and change the default boot image.

Before you begin

You must complete the downgrade preparation phase before you perform the downgrade procedures.

About this task

You can perform either a nondisruptive downgrade, in which the cluster remains online and continues to serve data during the downgrade, or a disruptive downgrade, in which the cluster is taken offline.

Choices

- [Downgrading a Data ONTAP cluster nondisruptively](#) on page 153
- [Downgrading a Data ONTAP cluster disruptively](#) on page 157

Downgrading a Data ONTAP cluster nondisruptively

The nondisruptive downgrade method has several steps: setting the default boot image for each node in the cluster, 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.

Before you begin

The cluster must consist of two or more nodes.

Steps

1. Verify that the target Data ONTAP 8.2 software is installed:

```
system node image show
```

Example

This example shows that version 8.2.0 is installed as the alternate image on both nodes.

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

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	8.2.1	11/25/2013 12:37:36
	image2	false	false	8.2.0	4/22/2013 13:52:22
node1	image1	true	true	8.2.1	11/25/2013 12:41:16
	image2	false	false	8.2.0	4/22/2013 13:55:22

4 entries were displayed.

For more information about installing the target Data ONTAP software image, see [Installing Data ONTAP 8.x software images in a cluster](#).

2. Change the current default boot image to 8.2.x:

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

This command identifies any functionality in the current release that is not supported in the earlier release. If any of these conditions are found, you must address them according to the instructions provided in the command output before you can proceed.

Example

This example shows that the default boot image will be changed to 8.2.0:

```
cluster1::> system node image modify {-iscurrent true} -isdefault false
2 entries were modified.
```

3. Redisplay the default boot image:

system node image show

Example

This example shows version 8.2.0 as the default image on both nodes:

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

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	false	true	8.2.1	11/25/2013 12:37:36
	image2	true	false	8.2.0	4/22/2013 13:52:22
node1	image1	false	true	8.2.1	11/25/2013 12:41:16
	image2	true	false	8.2.0	4/22/2013 13:55:22

4 entries were displayed.

4. Ensure that storage failover is enabled and possible:

storage failover show

Example

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

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

Node	Partner	Enabled	Takeover Possible	InterConn Up	State
node0	node1	true	true	true	connected
node1	node0	true	true	true	connected

2 entries were displayed.

5. If the cluster consists of only two nodes (a single HA pair), ensure that cluster HA is configured:

cluster ha show

Example

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

6. Disable automatic giveback on both nodes of the HA pair if it is enabled:

storage failover modify -node nodename -auto-giveback false

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

7. Migrate LIFs away from the node that will be taken over during the downgrade:

```
network interface migrate-all -node nodename
```

Data LIFs for SAN protocols are not migrated. As long as these LIFs exist on each node in the cluster, data can be served through alternate paths during the upgrade process.

8. Use the `network interface show` command to verify that the LIFs migrated away from the node.

Example

This 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      data005 node0      e0c      node1      e0c      up        up
vs0      data006 node0      e0d      node1      e0d      up        up
vs0      data007 node0      e0d      node1      e0d      up        up
vs0      data008 node0      e0c      node1      e0c      up        up
4 entries were displayed.
```

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

9. Initiate a takeover:

```
storage failover takeover -ofnode nodename
```

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

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 safely ignore this notification and proceed with the downgrade.

10. Verify that the takeover was successful:

```
storage failover show
```

Example

This example shows that the takeover was successful. Node node0 is in the `waiting for giveback` state, and its partner is `In takeover`.

```
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.
```

11. Wait 8 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 may take longer than 8 minutes depending on the characteristics of the client applications.

12. Return the root aggregate to the partner node:

storage failover giveback -ofnode nodename

Attention: The giveback is not initiated, an error message is returned, and an event is generated if any conditions such as the following are detected:

- Long-running operations (such as ASUP generation)
- Operations that cannot be restarted (such as aggregate creation)
- Error conditions (such as disk connectivity mismatch between the nodes)

If giveback is not initiated, complete the following steps:

- Address the "veto" condition described in the error message, ensuring that any identified operations are terminated gracefully.
- Reenter the giveback command:

storage failover giveback -ofnode nodename

Alternatively, you can analyze the messages and events for relevance to your environment. If you determine that the veto conditions are not significant, you can override the giveback veto by entering the following command:

storage failover giveback -ofnode nodename -override-vetoes true

For more information about determining whether you can safely override the veto, see the *Clustered Data ONTAP High-Availability Configuration Guide*.

This first returns the root aggregate to the partner node and then, after that node has finished booting, returns the non-root aggregates.

Before proceeding to the next step, ensure that all of the aggregates have been returned to node B. This process takes approximately 10 minutes.

13. Ensure that all of the aggregates have been returned:

storage failover show-giveback

After all of the aggregates are returned, the newly booted node begins to serve data to the clients.

14. Wait 8 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 may take longer than 8 minutes depending on the characteristics of the client applications.

15. Repeat Steps 7 on page 155 through 14 on page 156 on the other node in the HA pair.

16. Reenable automatic giveback on both nodes if it was previously enabled:

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

17. If you are downgrading a cluster that contains multiple HA pairs, ensure that the cluster is in quorum and that services are running before downgrading the next pair of nodes.

Downgrading a Data ONTAP cluster disruptively

If you can take your cluster offline to downgrade Data ONTAP, or if you have a single-node cluster, you can use the disruptive downgrade method. This method has several steps: disabling storage failover for each HA pair, updating the software on each node in the cluster, and then reenabling storage failover.

About this task

During a disruptive downgrade, each node acts as a single-node cluster. Any failures in the node will cause a data outage.

Steps

1. Verify that the target Data ONTAP 8.2 software is installed:

```
system node image show
```

Example

This example shows that version 8.2.0 is installed as the alternate image on both nodes.

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

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	8.2.1	11/25/2013 12:37:36
	image2	false	false	8.2.0	4/22/2013 13:52:22
node1	image1	true	true	8.2.1	11/25/2013 12:41:16
	image2	false	false	8.2.0	4/22/2013 13:55:22

4 entries were displayed.

For more information about installing the target Data ONTAP software image, see [Installing Data ONTAP 8.x software images in a cluster](#).

2. Change the current default boot image to 8.2.x:

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

This command identifies any functionality in the current release that is not supported in the earlier release. If any of these conditions are found, you must address them according to the instructions provided in the command output before you can proceed.

Example

This example shows that the default boot image will be changed to 8.2.0:

```
cluster1::> system node image modify {-iscurrent true} -isdefault false
2 entries were modified.
```

- 3. Redisplay the default boot image:

system node image show

Example

This example shows version 8.2.0 as the default image on both nodes:

```
cluster1::> system node image show
Node      Image  Is      Is      Version  Install
-----  -
node0     image1 false   true    8.2.1    11/25/2013 12:37:36
          image2 true    false   8.2.0    4/22/2013 13:52:22
node1     image1 false   true    8.2.1    11/25/2013 12:41:16
          image2 true    false   8.2.0    4/22/2013 13:55:22
4 entries were displayed.
```

- 4. Perform one of the following actions:

If the cluster consists of...	Do this...
One node	Continue to the next step.
Two nodes	<div>a. Disable cluster high availability: cluster ha modify -configured false</div> <div>b. Disable storage failover for the HA pair: storage failover modify -node * -enabled false</div>
More than two nodes	Disable storage failover for each HA pair in the cluster: storage failover modify -node * -enabled false

- 5. Reboot each node in the cluster:

system node reboot -node nodename

If the cluster consists of more than one node, you can reboot the nodes simultaneously.

Each node boots the new Data ONTAP image. The Data ONTAP login prompt appears, indicating that the reboot process is complete.

- When each node has rebooted with the new Data ONTAP image, confirm that the new Data ONTAP 8.2.x software is running:

```
system node image show
```

Example

This example shows version 8.2.1 as the current version on both nodes:

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

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	8.2.1	11/22/2013 13:52:22
	image2	false	false	8.1.2	10/25/2012 12:37:36
node1	image1	true	true	8.2.1	11/22/2013 13:55:22
	image2	false	false	8.1.2	10/25/2012 12:41:16

4 entries were displayed.

- Enable storage failover for each HA pair in the cluster:
storage failover modify -node * -enabled true
- If the cluster consists of two nodes, enable cluster high availability:
cluster ha modify -configured true

Completing post-downgrade tasks

After you downgrade the cluster to an earlier version of Data ONTAP 8.x, you should ensure that the cluster is functioning correctly.

Verifying that the cluster is in quorum

Before and after you perform an upgrade, reversion, or downgrade, you must ensure that all nodes are participating in a replicated database (RDB) quorum and that all rings are in the quorum. You must also verify that the per-ring quorum master is the same for all nodes.

About this task

For more information about cluster replication rings and RDB quorums, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

- Set the privilege level to advanced:
set -privilege advanced
Enter **y** to continue.
- Display each RDB process:

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 vldb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.1.x:

```
cluster1::*> cluster ring show -unitname vldb
```

Node	UnitName	Epoch	DB Epoch	DB Trnxs	Master
node0	vldb	154	154	14847	node0
node1	vldb	154	154	14847	node0
node2	vldb	154	154	14847	node0
node3	vldb	154	154	14847	node0

4 entries were displayed.

Example

This example shows the volume location database process for a cluster running Data ONTAP 8.2.x:

```
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.

For each process, verify the following configuration details:

- The relational database epoch and database epochs match for each node.
- The per-ring quorum master is the same for all nodes.

Note that each ring might have a different quorum master.

3. Return to the admin privilege level:

```
set -privilege admin
```

4. 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. During the upgrade, reversion, or downgrade process, each node will temporarily fall out

of SAN quorum. Therefore, if you are verifying the SAN quorum after completing an upgrade, reversion, or downgrade, you may notice critical event messages warning you that the nodes were previously out of SAN quorum.

If a node is out of SAN quorum, you can use the `storage failover takeover` and `storage failover giveback` commands to perform a planned takeover and giveback with the node's high-availability partner and bring the node back into SAN quorum.

Example

In this example, both nodes in the cluster are in SAN quorum.

```
cluster1::> event log show -messagename scsiblade.*
Time           Node      Severity      Event
-----
8/13/2013 14:03:51 node0      INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 14:03:51 node1      INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
```

Example

This example shows a two-node cluster after performing an upgrade. Each node shows a previous out of SAN quorum event message from when the node was upgraded. However, the most recent event message for each node shows that both nodes are presently in SAN quorum.

```
cluster1::> event log show -messagename scsiblade.*
Time           Node      Severity      Event
-----
8/13/2013 15:37:51 node1      INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:31:26 node1      CRITICAL      scsiblade.out.of.quorum: This node ...
8/13/2013 15:31:26 node1      INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:31:26 node1      INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:30:43 node0      INFORMATIONAL scsiblade.in.quorum: The scsi-blade ...
8/13/2013 15:24:16 node0      CRITICAL      scsiblade.out.of.quorum: This node ...
8/13/2013 15:24:16 node0      INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
8/13/2013 15:24:16 node0      INFORMATIONAL scsiblade.ics.trace.dumpfile: The ...
```

Verifying cluster and SVM health

Before and after you upgrade, revert, or downgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and the aggregates and volumes are online.

Steps

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster:

cluster show

Example

```
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. For more information about EMS messages, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

To troubleshoot cluster health issues, see the knowledgebase article [Troubleshooting Workflow: RDB app out of quorum](#) on the NetApp Support Site.

2. Determine if any disk drives are broken, undergoing maintenance, or reconstructing:

To check for...	Do this...
Broken disks	<p>a. Display any broken disks:</p> <pre>storage disk show -state broken</pre> <p>b. Remove or replace any broken disks.</p>
Disks undergoing maintenance or reconstructing	<p>a. Display any disks in maintenance, pending, or reconstructing states:</p> <pre>storage disk show -state maintenance pending reconstructing</pre> <p>b. Wait for the maintenance or reconstruction operation to complete before proceeding.</p>

3. To verify that all aggregates are online, display the state of physical and logical storage, including storage aggregates:

```
storage aggregate show -state !online
```

This command displays the aggregates that are *not* online.

Example

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

For more information about managing aggregates, see the *Clustered Data ONTAP Physical Storage Management Guide*.

4. To verify that all volumes are online, display any volumes *not* online:

```
volume show -state !online
```

Example

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

For more information about managing volumes, see the *Clustered Data ONTAP Logical Storage Management Guide*.

Enabling and reverting LIFs to home ports

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

About this task

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.

Steps

1. Display the status of all LIFs:

```
network interface show
```

Example

This example displays the status of all LIFs for a Storage Virtual Machine (SVM, formerly known as Vserver).

```
cluster1::> network interface show -vservers 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
```

Example

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

3. Revert LIFs to their home ports:

```
network interface revert *
```

Example

This command reverts all LIFs back to their home ports and changes all LIF home statuses to true.

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

- 4. Verify that all LIFs are in their home ports:

network interface show

Example

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.
```

Verifying client access (CIFS and NFS)

For the configured protocols, test access from CIFS and NFS clients to verify that the cluster is accessible.

Resuming SnapMirror operations

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

Before you begin

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

Steps

- 1. Resume transfers for each SnapMirror relationship that was previously quiesced:

snapmirror resume *

- 2. Verify that the SnapMirror operations have resumed:

snapmirror show

Example

```
cluster1::> snapmirror show
```

Source Path	Type	Destination Path	Mirror State	Relationship Status	Total Progress	Healthy	Last 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".

After you finish

For each SnapMirror relationship that is configured to run on a schedule, you should verify that the first scheduled SnapMirror transfer completes successfully.

Considerations for downgrading the SP firmware

If your current SP firmware version is not supported for the Data ONTAP release you are downgrading or reverting to, you must install a supported SP firmware version for the earlier Data ONTAP release.

After the Data ONTAP revert or downgrade process is complete, you must take the action to install an SP firmware version that is supported for the Data ONTAP version you reverted or downgraded to. To learn which SP firmware versions are supported by each Data ONTAP release, see the [BIOS Service Processor Support Matrix](#) on the NetApp Support Site. For instructions about downloading and installing an SP firmware version, see the [System Firmware and Diagnostics Download](#) page on the NetApp Support Site.

Reinstalling the required V-Series license after revert or downgrade

The licensing scheme for V-Series systems changed in Data ONTAP 8.2. Data ONTAP 8.2 and later requires the V_StorageAttach license package for V-Series systems to be able to access LUNs on storage arrays. Depending on the type of reversion you do, you might need to install the v-series license key for a prior release.

A license key is required for each V-Series system being reverted or downgraded.

If...	Then the V-Series license requirement is...
The V-Series system was upgraded to Data ONTAP 8.2 from the 8.1.x release family and you want to revert to a release in the 8.1.x release family again	You do not have to install the V-Series license for the release to which the system is being reverted. Data ONTAP remembers the V-Series license from when it was upgraded from 8.1.x to 8.2; Data ONTAP reinstalls those licenses when Data ONTAP is downgraded to 8.1.x.
Data ONTAP 8.2 is the first release of Data ONTAP installed on the system and you want to revert to a release in the 8.1.x release family	You must manually install the license key for V-Series systems that is supported for the release to which the system is being reverted. Contact your sales representative to obtain the appropriate license key for your system and release.
You want to downgrade the system from Data ONTAP 8.2.x to an earlier release in the 8.2 release family	You do not have to install the V_StorageAttach license package; Data ONTAP remembers the appropriate license for the release family.

For information about how to install licenses, see the *Clustered Data ONTAP System Administration Guide for SVM Administrators*.

Optimal service availability during upgrades

Service availability during Data ONTAP upgrades can be optimized through planning and configuration. In many cases, upgrades can be completely nondisruptive from a client perspective.

How upgrades impact service availability

You can review the factors that can affect the availability of cluster services before you begin the upgrade.

The following factors impact service availability:

- The types of protocols used and services licensed, and their susceptibility to timeout errors
- Whether you need to make decisions about Data ONTAP issues and new features between or within release families
Upgrading between Data ONTAP release families involves more steps and is potentially more disruptive than upgrades within a release family.
- Whether a system firmware update is required
Some system firmware updates require a system halt and reboot. This can disrupt services in upgrades when downtime is scheduled, but it does not affect services in nondisruptive upgrades.
- The types of applications in use and their susceptibility to timeout errors
The availability of client applications during upgrades depends on features, protocols, and configuration. See your application documentation for more information.

Note: All hardware and software upgrades in any storage solution are potentially at least somewhat disruptive to cluster services. Make sure that you review upgrade options carefully to determine the best method of upgrading for maintaining optimal service availability.

Related concepts

[Identifying potential upgrade issues](#) on page 24

[Updating firmware](#) on page 87

Considerations for services and protocols during upgrades

In general, services based on stateless protocols—such as NFS, FC, and iSCSI—are less susceptible to service interruptions during upgrades than session-oriented protocols—such as CIFS and NDMP.

During an upgrade, each node in the cluster must be rebooted (by initiating an HA configuration takeover and giveback) to load the new software. Services based on stateless protocols usually remain available during the nondisruptive upgrade.

Stateless protocols usually include a timeout procedure. For example, if a message is sent and receipt is not acknowledged within a timeout period, a transmission error is assumed to have occurred. In a cluster, if the client's timeout period is greater than the disruption period on the cluster (for example, the amount of time a reboot or HA configuration giveback takes), the client does not perceive a disruption of cluster services.

In session-oriented protocols, there is no concept of timeout to protect the service from disruption. If session-oriented cluster services are disrupted, state information about any operation in progress is lost and the user must restart the operation.

Considerations for stateless protocols

Configurations that include client connections using stateless NAS and SAN protocols generally do not experience adverse effects during upgrades if the clients are configured according to recommended guidelines.

If you are using stateless protocols, consider the following:

- **NFS hard mounts**
No adverse behavior is experienced on the clients during upgrade. Clients might receive some messages similar to the following until the node reboots:
`NFS server not responding, retrying`
In general, read/write directories should be hard-mounted. Hard mounts are the default type of mount.
- **NFS soft mounts**
You should not use soft mounts when there is a possibility of frequent NFS timeouts. Race conditions can occur as a result of these timeouts, which can lead to data corruption. Furthermore, some applications cannot properly handle errors that occur when an NFS operation reaches a timeout using soft mounts.
Situations that can cause frequent timeouts include nondisruptive upgrades or any takeover or giveback event in an HA configuration.
In general, soft mounts should be used only when reading solely from a disk; even then, understand that any soft mount is unreliable.
- **SAN protocols**
No adverse behavior is experienced on FC or iSCSI clients if they are configured according to recommended guidelines.
For more information, see the Interoperability Matrix on the NetApp Support Site.

Related information

[Interoperability Matrix: support.netapp.com/NOW/products/interoperability](https://support.netapp.com/NOW/products/interoperability)

Considerations for session-oriented protocols

Clusters and session-oriented protocols might cause adverse effects on clients and applications in certain areas during upgrades.

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

- CIFS
Hyper-V over SMB supports nondisruptive operations (NDO). If you configured a Hyper-V over SMB solution, Hyper-V and the contained virtual machines remain online and provide continuous availability during the Data ONTAP upgrade.
For all other CIFS configurations, client sessions are terminated. You should direct users to end their sessions before you upgrade.
- NDMP
State is lost and the client user must retry the operation.
- Backups and restores
State is lost and the client user must retry the operation.

Attention: Do not initiate a backup or restore during or immediately before an upgrade. Doing so might result in data loss.
- Applications (for example, Oracle or Exchange)
Effects depend on the applications. For timeout-based applications, you might be able to change the timeout setting to longer than the Data ONTAP reboot time to minimize adverse effects.

Understanding background disk firmware updates

When a node reboots and there is new disk firmware present, the affected drives are automatically and sequentially taken offline, and the node responds normally to read and write requests.

If any request affects an offline drive, the read requests are satisfied by reconstructing data from other disks in the RAID group, while write requests are written to a log. When the disk firmware update is complete, the drive is brought back online after resynchronizing any write operations that took place while the drive was offline.

During a background disk firmware update, the node functions normally. You see status messages as disks are taken offline to update firmware and brought back online when the firmware update is complete. Background disk firmware updates proceed sequentially for active data disks and for spare disks. Sequential disk firmware updates ensure that there is no data loss through double-disk failure.

Offline drives are marked with the annotation `offline` in the nodeshell `vol status -r` command output. While a spare disk is offline, it cannot be added to a volume or selected as a replacement drive for reconstruction operations. However, a disk would normally remain offline for a very short time (a few minutes at most) and therefore would not interfere with normal cluster operation.

The background disk firmware update is completed unless the following conditions are encountered:

- Degraded aggregates are on the node.
- Disks needing a firmware update are present in an aggregate or plex that is in an offline state.

Automatic background disk firmware updates resume when these conditions are addressed. For more information about determining aggregate status and state, see the *Clustered Data ONTAP Physical Storage Management Guide*.

Upgrading Data ONTAP-v systems

Upgrading Data ONTAP software on platforms based on Data ONTAP-v technology, for example, the Data ONTAP Edge product, requires a few additional preparatory steps.

Platforms that are based on Data ONTAP-v technology run standard Data ONTAP software, but like some of the hardware platforms that run Data ONTAP, the image you must download is unique.

Important: Data ONTAP Edge 7-Mode systems cannot be upgraded with clustered Data ONTAP software.

Upgrade process overview for Data ONTAP-v systems

Before beginning to upgrade Data ONTAP software, you should plan the upgrade and familiarize yourself with the required steps.

1. Plan your upgrade by familiarizing yourself with requirements and issues before you upgrade:
 - Review the *Release Notes* for your upgrade target release.
 - Understand any requirements for upgrading to the target release from your existing software.
 - Create a back-out plan, in the unlikely event that you need to revert or downgrade to the Data ONTAP release that was running on your system before the upgrade.
 - Note any potential changes to your system after the upgrade.
 - If you run the SnapMirror software, identify storage systems with destination and source volumes.
2. If necessary, perform any required preparatory procedures before upgrading to the new Data ONTAP release:
 - Verify that any versions of VMware vSphere are compatible with your upgrade target release. If the new version of Data ONTAP software requires new vSphere software, upgrade the vSphere software first.
For more information about software compatibility, see the *Release Notes* and the Interoperability Matrix for your Data ONTAP upgrade target release.
 - Ensure that you have a current Snapshot copy of the root volume of any system being upgraded.
3. Obtain the appropriate software image from the NetApp Support Site.
Copy the image to your storage system or to an HTTP server on your network.
4. Install the Data ONTAP software image on your storage system.
Extract the system files from the software image you copied to your system.
5. Download the new Data ONTAP system files to the boot device.
The upgrade process is finished when your system reboots with the new version of Data ONTAP.

6. Verify that the version of dvadmin (the Data ONTAP-v administration tool) is compatible with your upgrade target release.
See the *Release Notes* and the Interoperability Matrix for your Data ONTAP upgrade target release.
If you need to upgrade dvadmin, you should install the upgrade after the new version of Data ONTAP has been installed. For dvadmin upgrade instructions, see the *Data ONTAP-v Administration Tool Installation Guide*.
7. Verify that your systems are operating as expected after the upgrade.
Before returning storage systems to production, you should check the status of configured functionality and re-enable any functionality that was suspended before the upgrade.

Related information

Download Software: support.netapp.com/NOW/cgi-bin/software

NetApp Interoperability Matrix: support.netapp.com/NOW/products/interoperability

Recommendations for Data ONTAP-v systems upgrading to this release

You should follow these simple guidelines to ensure your storage system upgrade is successful.

- Review the "Important cautions" section of the Release Notes for this Data ONTAP release. It contains important information that could affect the behavior of your system during and after upgrading.
- Upgrade during non-peak hours.
- Avoid performing a quota initialization prior to upgrading.
If a quota initialization is in process prior to upgrading, wait for the initialization to finish.

Preparing for a Data ONTAP-v system upgrade

Before installing the latest Data ONTAP release on your storage system, you need to verify information and complete some tasks.

Steps

1. Verify that your system meets the minimum requirements.
For more information about system requirements, see the Release Notes for your Data ONTAP upgrade target release.
2. Create a backup of Data ONTAP-v system information, including the virtual machine configuration and all of the information on the Data ONTAP-v system disks, by entering the following dvadmin command:

`vm config backup <vm_name> <backup_name>`
3. Connect to the storage system and confirm that all paths to disks are visible to the system by entering the following Data ONTAP command:

```
storage disk show
```

4. Confirm that there are no failed disks by entering the following command:

```
storage disk show -state broken
```

5. Verify that all aggregates are online by entering the following command:

```
storage aggr show
```

6. Ensure that a recent cluster configuration backup file has been created and uploaded to a remote server. You can use the `system configuration backup` command for this purpose. This information can be used to recover the cluster's configuration if the node is corrupted.
7. Ensure that you have a current Snapshot copy of the root volume of any system being upgraded.

For more information about creating Snapshot copies, see the *Clustered Data ONTAP Data Protection Guide*.

8. If you are running SnapMirror, identify storage systems with destination volumes and upgrade them before upgrading storage systems with source volumes.

Obtaining software images for Data ONTAP-v systems

To upgrade the storage system to the latest release of Data ONTAP, you need access to software images. Software images are available on the NetApp Support Site.

You can copy software images to an HTTP server on your network and then Data ONTAP-v storage systems can access the images by using the `system node image` command.

Software images are specific to storage system models. Be sure to obtain the correct image for your system.

Related information

[Download Software: support.netapp.com/NOW/cgi-bin/software](https://support.netapp.com/NOW/cgi-bin/software)

Copying the software image to the HTTP server

If you have an HTTP server that is accessible to your storage system, you can copy Data ONTAP software images to the HTTP server. This task prepares the HTTP server to serve software images to storage systems in your environment.

Steps

1. Locate the Data ONTAP software in the Data ONTAP Edge Software Downloads area of the NetApp Support Site.
2. Copy the software image (for example, `821_v_image.tgz`) from the NetApp Support Site to the directory on the HTTP server from which the file is served.

Copying the software image from the HTTP server to the storage system

You can copy software images to the `/etc/software` directory of your storage system if you plan to perform the installation later. If you want to copy the image and perform the installation in one step, see the section on Installing Software Images.

Step

1. Enter the following command from the storage system console:

```
system node image get -package url
```

url is the URL that provides the location of the package to be fetched. Standard URL schemes, including HTTP, FTP, TFTP and FILE, are accepted.

Use the following URL syntax if you need to specify a user name, password, host, and port to access files on the HTTP server using Basic Access Authentication (RFC2617):

```
http://username:password@host:port/path
```

Example

In the following example, the `system node image get` command copies the file `821_v_image.tgz` to the storage system:

```
system node image get -package http://www.example.com/downloads/  
x86-64/821_v_image.tgz
```

You see a message similar to the following:

```
software: copying to /etc/software/821_v_image.tgz  
software: 100% file read from location.  
software: /etc/software/821_v_image.tgz has been copied.
```

Installing software images on Data ONTAP-v systems

You use the `system node image update` command to extract and install new Data ONTAP software images on your storage system.

You must know the location of and have access to the software image. The `system node image update` command requires one of the following as an argument:

- The path to a software image in a mounted file system in the form "file://localhost/path_to_file". For example, `file://localhost/mroot/etc/software/821_v_image.tgz`.
- The URL that provides the location of the package to be downloaded. Standard URL schemes, including HTTP, FTP, and TFTP, are accepted.

The `system node image update` command allows you to perform several operations at one time. For example, you can use a single command to copy an image from the HTTP server, extract and install the system files, download the files to the boot device, and reboot your system.

For more information about the `system node image update` command and its options, see the appropriate man page.

Installing software images

You can install software from an HTTP server or from a software image you copied to the storage system.

Step

1. From the storage system prompt, enter the following command:

```
system node image update {url/file_name} options
```

- *url* is the URL of the HTTP server, subdirectory, and file name.
- *file_name* is the name of the file you copied to the `/etc/software` directory.
- *options* are one or more of the following:
 - The `-replace-package` option overwrites the existing image in the `/etc/software` directory when you install software from an HTTP server.
 - The `-setdefault` option specifies whether to set the newly updated image as the default image, that is, the image that runs the next time the node is restarted.

Example

Enter the following command to update the software image on the current node from a software package located at `ftp://ftp.example.com/downloads/821_v_image.tgz`:

```
system node image update -package ftp://ftp.example.com/downloads/  
821_v_image.tgz -setdefault
```

Verifying Data ONTAP-v system status after an upgrade

It is a best practice to verify that upgraded systems are functioning as expected before returning them to production. This entails verifying the status of configured functionality and re-enabling any functionality that was suspended before the upgrade.

About this task

These tasks should be performed on each system that was upgraded.

Steps

1. Verify that the intended target release is installed and running by entering the following command:


```
version
```
2. Confirm that all paths to disks are visible to the system by entering the following command:

```
storage disk show
```

3. Confirm that there are no failed disks by entering the following command:

```
storage disk show -state broken
```

4. Verify that all aggregates are online by entering the following command:

```
storage aggr show
```

5. Confirm that network interfaces are online by entering the following command:

```
network port show
```

6. If you quiesced SnapMirror transfers, enter the following command for each destination volume to resume them:

```
snapmirror resume destination
```

After you finish

If the new Data ONTAP version requires that you upgrade the dvadmin software, you should install the new Data ONTAP-v Installer virtual machine and dvadmin software at this time. See the *Data ONTAP-v Administration Tool Installation Guide* for upgrade instructions.

Copyright information

Copyright © 1994–2014 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, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Customer Fitness, Cryptainer, CryptoShred, CyberSnap, Data Center Fitness, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, ExpressPod, FAServer, FastStak, FilerView, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, Snap Creator, SnapDirector, SnapDrive, SnapFilter, SnapIntegrator, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, VelocityStak, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

A

- ACP firmware
 - updates to [91](#)
- aggregates
 - deduplicated, verifying space for [29](#)
 - verifying status [33](#), [78](#), [102](#), [128](#), [141](#), [161](#)
- Alternate Control Path
 - See* ACP
- alternate image
 - bootable [43](#)
- AutoSupport
 - detecting outdated disk firmware using [89](#)

B

- back-end configurations
 - finding errors before downgrading [146](#)
- background disks
 - understanding firmware updates for [169](#)
- back-out plans
 - for Data ONTAP-v upgrades [170](#)
- Baseboard Management Controller
 - See* BMC
- basic input/output
 - See* BIOS
- batch upgrades
 - definition of [11](#)
 - disabling automatic LIF rebalancing before [37](#)
 - enabling automatic LIF rebalancing after [86](#)
 - process for [61](#)
 - upgrades
 - upgrading the first set of nodes using the batch method [62](#)
 - upgrading the second set of nodes using the batch method [68](#)
 - verifying for batches using the batch method [73](#)
 - upgrading the first set of nodes [62](#)
 - upgrading the second set of nodes [68](#)
 - verifying cluster version [76](#)
 - verifying completion of [73](#)
 - verifying the cluster is ready for [48](#)
- boot images
 - checking before an upgrade [11](#)
- BranchCache
 - requirement for disabling before reverting [115](#)

C

- checklists
 - downgrade [135](#)
 - reversion [95](#)
 - upgrade [11](#)
- CIFS
 - avoiding interruptions during upgrades [168](#)
 - identifying active sessions before downgrading [38](#), [144](#)
 - identifying active sessions before upgrading [38](#), [144](#)
 - requirement for reconfiguring IPv6 addresses before reverting [112](#)
 - verifying client access for [131](#), [164](#)
- CIFS servers
 - actions you must take for local user and group configurations before reverting [114](#)
- cluster
 - verifying system time is synchronized [40](#), [118](#), [145](#)
- cluster health
 - verifying [33](#), [78](#), [102](#), [128](#), [141](#), [161](#)
- cluster management LIF
 - configuring RSA [83](#)
- cluster peer relationships
 - deleting before reverting [110](#)
- cluster replication rings
 - verifying cluster is in RDB quorum [31](#), [76](#), [100](#), [126](#), [139](#), [159](#)
- cluster version
 - verifying after upgrade [76](#)
- clusters
 - checking status [11](#)
 - disruptive upgrades [74](#)
 - downgrade process for [152](#)
 - downgrades
 - checklist for [135](#)
 - completing post-downgrade tasks [159](#)
 - issues for [138](#)
 - to earlier release in same release family, overview of [134](#)
 - downgrading disruptively [157](#)
 - downgrading nondisruptively [153](#)
 - ensuring that no jobs are running before upgrading or downgrading [46](#), [151](#)
 - how images are stored and alternated [43](#)
 - installing software images [42](#), [121](#), [148](#)

preparing to revert, SnapMirror and SnapVault relationships [104](#)

reversions

checklist for [95](#)

completing post-reversion tasks for [126](#)

issues and limitations [98](#)

reverting to an earlier release family, overview [94](#)

reverting to a previous release

required tasks when preparing for [100](#)

reverting with no I/O [123](#)

upgrades

checklist for [11](#)

planning [10](#)

process for [47](#)

process overview [8](#)

verifying CIFS and NFS client access for [131](#), [164](#)

verifying cluster is in RDB quorum [31](#), [76](#), [100](#), [126](#), [139](#), [159](#)

verifying health [33](#), [78](#), [102](#), [128](#), [141](#), [161](#)

commands

RSA setup [83](#)

software update [173](#)

system node image show

determining software version before

downgrading [147](#)

determining software version before upgrading [41](#)

system node revert-to [94](#)

Common Internet File System

.See CIFS

compressed volumes

reversion requirements [116](#)

Config Advisor

checking for common configuration errors with [28](#)

downloading and running [28](#)

configuration requirements

for upgrades [17](#)

configurations

errors in back-end [146](#)

considerations

for downgrading the SP firmware [132](#), [165](#)

D

Data ONTAP

downgrading nondisruptively [153](#)

installing Data ONTAP-v software images [173](#)

overview of upgrade process [8](#)

potential 8.2 upgrade issues [24](#)

reverting to an earlier release family, overview [94](#)

upgrading nondisruptively in SnapMirror

environments [45](#), [150](#)

Data ONTAP 8.2 release family

changes to behavior [26](#)

Data ONTAP software images

how images are stored and alternated [43](#)

obtaining [41](#), [121](#), [148](#)

required tasks when preparing to revert [100](#)

Data ONTAP system files

copying the software image to the HTTP server [172](#)

Data ONTAP-v

preparing for the upgrade [171](#)

recommendations for upgrading [171](#)

upgrade overview [170](#)

upgrade planning [8](#)

verifying system status after upgrading [174](#)

Data ONTAP-v software images

copying to the storage system [173](#)

installing from an HTTP server [174](#)

obtaining [172](#)

data protection mirror

relationships, before reverting a cluster [104](#)

data protection mirror relationships

considerations for updating after upgrades [22](#)

deleting before reverting [104](#), [106](#)

data protection mirrors

upgrading older style relationships [84](#)

deduplicated volumes

reverting systems with [115](#)

deduplication

verifying space for before upgrading [29](#)

default boot images

checking before an upgrade [11](#)

deleting

SVMs with Infinite Volume [118](#)

disk firmware

about updating [87](#)

detecting outdated, using AutoSupport [89](#)

service availability during updates [89](#)

understanding background updates for [169](#)

Disk Qualification Package

when you need to update [88](#)

disk shelf firmware updates

about [90](#)

disk shelves

about updating firmware for [87](#)

ACP updates for [91](#)

detecting outdated firmware [91](#)

firmware updates for, about [90](#)

- how firmware is updated [90](#)
- disks
 - about updating firmware for [87](#)
 - detecting outdated firmware [89](#)
 - how firmware is updated during upgrades [87](#)
 - service availability during firmware updates [89](#)
 - understanding background firmware updates for [169](#)
- disruptive downgrades
 - procedure for [157](#)
- disruptive upgrades
 - definition of [11](#)
 - procedure for [74](#)
 - verifying that the cluster is ready for [48](#)
- downgrades
 - checklist for [135](#)
 - completing post-downgrade tasks [159](#)
 - deleting Infinite Volumes [118](#)
 - determining software version [147](#)
 - disruptive, procedure for [157](#)
 - downgrade issues [138](#)
 - enabling and reverting LIFs to home ports, before and after [34](#), [80](#), [129](#), [143](#), [163](#)
 - finding back-end configuration errors before downgrading [146](#)
 - identifying issues when [139](#)
 - nondisruptive, procedure for [153](#)
 - overview of, to earlier release in same release family [134](#)
 - prerequisites for V-Series systems [138](#)
 - process for [152](#)
 - requirements for planning [134](#)
 - Storage Encryption restriction for [138](#)
 - when to call technical support [134](#)
- downgrading to a previous release
 - V-Series licensing requirement [132](#), [165](#)
- DQP
 - See* Disk Qualification Package
- drives
 - when you need to update the Disk Qualification Package [88](#)
- dump operations
 - verifying job status before upgrading or downgrading [46](#), [151](#)

E

- errors
 - finding before downgrading [146](#)
- export policies

- requirement for configuring for SMB access before reverting [114](#)

F

- File Transfer Protocol
 - See* FTP
- firmware
 - about updating disk, shelf, and system [87](#)
 - about updating Flash Cache [92](#)
 - about updating for disks [87](#)
 - about updating PAM [92](#)
 - considerations for downgrading the SP [132](#), [165](#)
 - detecting outdated disk, using AutoSupport [89](#)
 - detecting outdated, for disk shelves [91](#)
 - disk shelf, update process overview [90](#)
 - disk, how updated [87](#)
 - RLM, updates to [92](#)
 - updating system, about [87](#)
- firmware updates
 - about SP [92](#)
 - ACP [91](#)
 - disk shelf, about [90](#)
 - service availability during disk [89](#)
 - understanding background disk [169](#)
- Flash Cache
 - about updating firmware [92](#)
- FPolicy
 - actions you must take before reverting [112](#)

H

- HTTP servers
 - copying the software image [172](#)
 - installing Data ONTAP-v software images [174](#)
- Hyper-V over SMB
 - actions you must take before reverting [113](#)

I

- images
 - See* software images
- Infinite Volumes
 - considerations for upgrade [22](#)
 - creating namespace mirror constituents after upgrade [81](#)
 - deleting [118](#)
- installing Data ONTAP software images
 - from an HTTP server [174](#)
- IPv6 for CIFS

requirement for reconfiguring before reverting [112](#)
 issues
 downgrade [138](#), [139](#)
 evaluating potential upgrade [24](#)
 potential Data ONTAP 8.2 release family upgrade [24](#)
 reversion [98](#), [99](#)

J

jobs
 verifying status before upgrading or downgrading [46](#), [151](#)

L

licensing
 V-Series requirement when downgrading [132](#), [165](#)
 V-Series requirement when reverting [132](#), [165](#)
 LIFs
 disabling automatic rebalancing for [37](#)
 enabling and reverting to home ports [34](#), [80](#), [129](#), [143](#), [163](#)
 enabling automatic rebalancing for [86](#)
 setting up Remote Support Agent [83](#)
 verifying the failover configuration for [36](#)
 limitations
 downgrade [138](#)
 reversion [98](#)
 limits
 for cluster upgrades [18](#)
 load-sharing mirror
 relationships, before reverting a cluster [104](#)
 load-sharing mirror relationships
 deleting before reverting [104](#)
 local users and groups
 SMB, actions you must take before reverting [114](#)
 logical interfaces
 See LIFs
 low memory system [24](#)

M

major nondisruptive upgrades
 disk shelf firmware update requirement [90](#)
 mirror relationships
 deleting before reverting [104](#), [106](#)
 mirroring
 See SnapMirror environments
 mixed version requirements
 for upgrades [17](#)

module firmware
 disk shelf, update process overview [90](#)
 updating SP, about [92](#)

N

namespace mirror constituents
 considerations for creating after upgrades [22](#)
 creating for Infinite Volumes after upgrading [81](#)
 NDMP
 avoiding interruptions during upgrades [168](#)
 NDUs
 See nondisruptive upgrades
 NetApp Interoperability Matrix
 upgrading Data ONTAP [170](#)
 NetApp Support Site
 obtaining Data ONTAP software images [41](#), [121](#), [148](#), [172](#)
 Network Data Management Protocol
 See NDMP
 Network File System
 See NFS
 NFS
 protocol considerations for upgrades [168](#)
 verifying client access for [131](#), [164](#)
 nodes
 identifying software version [41](#), [147](#)
 sequence for upgrading [19](#)
 verifying participation in RDB quorums [31](#), [76](#), [100](#), [126](#), [139](#), [159](#)
 nondisruptive downgrades
 procedure for [153](#)
 nondisruptive upgrades
 about optimizing service availability during [167](#)
 avoiding service interruptions during [167](#)
 batch method for [61](#)
 definition of [11](#)
 disk shelf firmware, about [90](#)
 estimating the duration of [22](#)
 how updating Flash Cache firmware works [92](#)
 methods for [11](#)
 resuming SnapMirror operations after [84](#), [164](#)
 rolling upgrade method for [49](#)
 sequence for upgrading nodes [19](#)
 SnapMirror environment, steps for [45](#), [150](#)
 verifying that the cluster is ready for [48](#)

O

obtaining

- Data ONTAP software images [41](#), [121](#), [148](#)
- outdated firmware
 - detecting, for disk shelves [91](#)
 - detecting, for disks [89](#)
- overview
 - downgrade to earlier release in same release family [134](#)
 - upgrade process [8](#)

P

- PAM
 - about updating firmware [92](#)
- peer relationships
 - deleting cluster, before reverting [110](#)
 - deleting SVM, before reverting [109](#)
- Performance Acceleration Module
 - See* PAM
- performance baselines
 - establishing with Perfstat before upgrade [30](#)
- performing upgrades
 - checklist for [11](#)
 - process for [47](#)
- Perfstat
 - creating performance baseline with, before upgrading [30](#)
- planning
 - requirements for downgrades [134](#)
 - reversions [95](#)
 - upgrades [10](#)
 - upgrades with Upgrade Advisor [9](#)
- post-downgrade tasks
 - checklist for [135](#)
 - completing [159](#)
- post-reversion tasks
 - checklist for [95](#)
 - completing [126](#)
- post-upgrade tasks
 - checklist for [11](#)
 - verifying system status [174](#)
- pre-downgrade tasks
 - checklist for [135](#)
- pre-reversion tasks
 - checklist for [95](#)
- pre-upgrade tasks
 - checklist for [11](#)
- preparing
 - for Data ONTAP-v upgrades [171](#)
 - required tasks for reversions [100](#)
- production clusters

- preparing to revert [104](#)
- protocols
 - avoiding interruptions during upgrades [167](#)
 - considerations for session-oriented [168](#)
 - upgrade considerations for stateless [168](#)

Q

- quorum
 - verifying the cluster is in [31](#), [76](#), [100](#), [126](#), [139](#), [159](#)

R

- relationships
 - deleting cluster peer, before reverting [110](#)
 - deleting data protection mirror, before reverting [106](#)
 - deleting mirror, before reverting [104](#)
 - deleting SnapVault, before reverting [108](#)
 - deleting SVM peer, before reverting [109](#)
 - upgrading older style SnapMirror [84](#)
- release families
 - changes to behavior in Data ONTAP 8.2 [26](#)
 - evaluating potential upgrade issues [24](#)
 - impact of upgrades on service availability [167](#)
- release requirements
 - for upgrades [17](#)
- remote LAN module
 - See* RLM
- Remote Support Agent
 - setting cluster management LIF after upgrading [83](#)
- replicated database quorums
 - See* RDB quorums
- replication rings
 - verifying cluster is in RDB quorum [31](#), [76](#), [100](#), [126](#), [139](#), [159](#)
- requirements
 - downgrade planning [134](#)
 - for cluster upgrades [17](#)
 - SnapMirror upgrade [23](#)
 - verifying job status before upgrading or downgrading [46](#), [151](#)
- restore operations
 - verifying job status before upgrading or downgrading [46](#), [151](#)
- reversion issues
 - considerations about [98](#)
 - deleting load-sharing and data-protection mirror relationships [104](#)
 - identifying [99](#)
- reversions

enabling and reverting LIFs to home ports, after [34](#), [80](#), [129](#), [143](#), [163](#)

with no I/O, procedure for [123](#)

revert operations

actions you must take for FPolicy configurations before performing [112](#)

actions you must take for Hyper-V over SMB before performing [113](#)

actions you must take for SMB local users and groups before performing [114](#)

deleting cluster peer relationships before performing [110](#)

deleting data protection mirror relationships before performing [106](#)

deleting peer relationships before performing [109](#)

deleting SnapVault relationships before performing [108](#)

requirement for configuring export policies for SMB access before performing [114](#)

requirement for disabling BranchCache before performing [115](#)

requirement for disabling SMB 3.0 before performing [111](#)

requirement for reconfiguring CIFS IPv6 addresses before performing [112](#)

reverting to a previous release

checklist for [95](#)

compressed volumes [116](#)

deduplicated volumes [115](#)

deleting Infinite Volumes [118](#)

deleting mirror relationships [104](#)

identifying issues when [98](#), [99](#)

overview of requirements [95](#)

post-reversion tasks for [126](#)

preparing for production clusters [104](#)

preparing Snapshot copies after [131](#)

preparing Snapshot copies before [119](#)

required tasks when preparing for [100](#)

supported scenarios for [94](#)

V-Series licensing requirement [132](#), [165](#)

when to call technical support [94](#)

RLM

about updating firmware [92](#)

rolling upgrades

definition of [11](#)

process for [49](#)

upgrades

upgrading the first node using the rolling method [50](#)

upgrading the second node using the rolling method [55](#)

verifying for HA pairs using the rolling method [60](#)

upgrading the first node [50](#)

upgrading the second node [55](#)

verifying cluster version [76](#)

verifying for HA pairs [60](#)

verifying that the cluster is ready for [48](#)

RSA

See Remote Support Agent

RSA setup command

setting up Remote Support Agent [83](#)

S

SAN

protocol considerations for upgrades [168](#)

service availability

about optimizing during upgrades [167](#)

avoiding interruptions during upgrades [167](#)

during disk firmware updates [89](#)

impact of upgrades on [167](#)

Service Processor

See SP firmware

session-oriented protocols

avoiding service interruptions during upgrades [168](#)

shelves

detecting outdated firmware for [91](#)

how firmware is updated [90](#)

Simple Network Management Protocol

See SNMP

single-node clusters

downgrading [157](#)

upgrading [74](#)

SMB 3.0

requirement for disabling before reverting [111](#)

SMB access

requirement for export policies to be configured before reverting [114](#)

SMB local users and groups

actions you must take before reverting [114](#)

SnapMirror environments

identifying destination volumes [170](#)

resuming operations after NDU [84](#), [164](#)

upgrade requirements for [23](#)

upgrading nondisruptively [45](#), [150](#)

SnapMirror relationships

upgrading older style [84](#)

Snapshot copies

- deleting copies with compressed data before reverting [116](#)
 - preparing after reverting [131](#)
 - preparing before reverting [119](#)
 - preparing for the upgrade [170](#), [171](#)
 - SnapVault
 - relationships, before reverting a cluster [104](#)
 - SnapVault relationships
 - deleting before reverting [108](#)
 - software images
 - about [172](#)
 - copying [41](#), [121](#), [148](#), [172](#)
 - Data ONTAP-v [173](#)
 - how images are stored and alternated [43](#)
 - installing [42](#), [121](#), [148](#), [173](#), [174](#)
 - required tasks when preparing to revert [100](#)
 - software update command
 - installing software images [173](#)
 - software versions
 - identifying before downgrade [147](#)
 - identifying before upgrade [41](#)
 - SP firmware
 - about updating [92](#)
 - considerations for downgrading the [132](#), [165](#)
 - stateless protocols
 - avoiding service interruptions during upgrades [168](#)
 - storage area network
 - See* SAN
 - Storage Encryption
 - downgrade restriction [138](#)
 - storage systems
 - compatibility with Data ONTAP [170](#)
 - upgrading mirrored environment nondisruptively [45](#), [150](#)
 - support
 - when to call during downgrade [134](#)
 - when to call during revert [94](#)
 - SVM health
 - verifying [33](#), [78](#), [102](#), [128](#), [141](#), [161](#)
 - SVMs
 - deleting Infinite Volumes [118](#)
 - deleting peer relationships of, before reverting [109](#)
 - verifying health [33](#), [78](#), [102](#), [128](#), [141](#), [161](#)
 - system files, Data ONTAP
 - copying software images [172](#)
 - copying the software images [41](#), [121](#), [148](#)
 - system files, Data ONTAP-v
 - installing [174](#)
 - system firmware
 - installing automatically, about [87](#)
 - system limits
 - See* limits
 - system node image show command
 - determining software version [41](#), [147](#)
 - system node revert-to command
 - reverting Data ONTAP [94](#)
 - system services
 - verifying after a reversion [126](#)
 - system status
 - verifying after an upgrade [174](#)
 - system time
 - verifying [40](#), [118](#), [145](#)
- ## T
- technical support
 - when to call during downgrade [134](#)
 - when to call during revert [94](#)
 - troubleshooting
 - reverting LIFs to home ports [34](#), [80](#), [129](#), [143](#), [163](#)
- ## U
- updates
 - disk firmware, about [87](#)
 - disk shelf firmware, about [90](#)
 - disk shelf firmware, overview [90](#)
 - Flash Cache firmware, about [92](#)
 - how disk firmware is updated [87](#)
 - RLM firmware overview [92](#)
 - service availability during disk firmware [89](#)
 - SP firmware, about [92](#)
 - system firmware, about [87](#)
 - understanding background disk firmware [169](#)
 - upgrade
 - creating namespace mirror constituents on Infinite Volumes [81](#)
 - Upgrade Advisor tool
 - planning your upgrade with [9](#)
 - upgrades
 - about maintaining service availability during [167](#)
 - avoiding service interruptions [167](#)
 - checklist for [11](#)
 - considerations with session-oriented protocols [168](#)
 - considerations with stateless protocols [168](#)
 - creating performance baseline before [30](#)
 - Data ONTAP 8.2 changes to behavior [26](#)
 - determining software version [41](#)
 - enabling and reverting LIFs to home ports, before and after [34](#), [80](#), [129](#), [143](#), [163](#)

- estimating the duration of [22](#)
- evaluating potential issues [24](#)
- how disk firmware is updated for [87](#)
- how disk shelf firmware is updated [90](#)
- impact on service availability [167](#)
- limits for [18](#)
- obtaining Data ONTAP software images [41](#), [121](#), [148](#)
- planning for [10](#)
- planning with Upgrade Advisor [9](#)
- potential issues with Data ONTAP 8.2 release family [24](#)
- procedure for disruptive [74](#)
- process for performing [47](#)
- process overview [8](#), [171](#)
- recommendations for Data ONTAP-v systems [171](#)
- requirements for [17](#)
- requirements for SnapMirror [23](#)
- sequence for upgrading nodes [19](#)
- SnapMirror environment, nondisruptive steps [45](#), [150](#)
- system firmware, about [87](#)
- types of [11](#)
- verifying cluster is in RDB quorum before [31](#), [76](#), [100](#), [126](#), [139](#), [159](#)
- verifying cluster version [76](#)
- verifying system status after [174](#)
- verifying that the cluster is ready for [48](#)
- upgrading [24](#)
- utilities

- checking for common configuration errors with Config Advisor [28](#)
- downloading and running Config Advisor [28](#)

V

- V-Series systems
 - finding errors before downgrading [146](#)
 - prerequisites for downgrading [138](#)
- verifying
 - cluster is in quorum [31](#), [76](#), [100](#), [126](#), [139](#), [159](#)
- versions
 - detecting outdated disk firmware [89](#)
 - detecting outdated disk shelf firmware [91](#)
 - identifying current software [147](#)
 - identifying current software on nodes [41](#)
- volumes
 - deduplicated, verifying space for [29](#)
 - verifying status [33](#), [78](#), [102](#), [128](#), [141](#), [161](#)
 - verifying volume status before upgrading or downgrading [46](#), [151](#)
- vsadmin role
 - enabling after a revert operation
 - enabling
 - vsadmin role after a revert operation [133](#)
- Vservers
 - See* SVMs