Clustered Data ONTAP® 8.3

Upgrade and Revert/Downgrade Guide

January 2016 | 215-10117_B0
doccomments@netapp.com

Updated for 8.3.1
# Contents

**Upgrading Data ONTAP clusters** .......................................................... 6
- Cluster upgrade workflow ........................................................................ 6
- Cluster upgrade checklist ........................................................................ 7
- Types of cluster upgrades ....................................................................... 17
- Planning an upgrade to a Data ONTAP Edge storage system .................. 18
- Planning your upgrade with Upgrade Advisor ........................................ 19
- Planning your upgrade ........................................................................... 20
  - Reviewing pre-upgrade resources ..................................................... 21
  - Reviewing cluster upgrade requirements .......................................... 21
  - Verifying cluster upgrade limits ......................................................... 28
  - Planning the upgrade sequence for a batch upgrade ......................... 29
  - Creating a performance baseline with Perfsat Converged ................. 30
- Preparing for a Data ONTAP cluster upgrade ........................................ 31
  - Verifying that the cluster is ready to be upgraded ......................... 31
  - Preparing Data ONTAP features for the upgrade ............................ 43
  - Obtaining Data ONTAP software images ...................................... 55
  - Installing Data ONTAP software images for a major upgrade .......... 56
  - Disabling the 32-bit capability ......................................................... 59
- Performing the software upgrade .......................................................... 62
  - Upgrading a Data ONTAP cluster nondisruptively by using the rolling
    upgrade method ............................................................................... 62
  - Upgrading a Data ONTAP cluster nondisruptively by using the batch
    method ......................................................................................... 73
  - Upgrading a Data ONTAP cluster nondisruptively by using the
    automated method (minor NDU only) ............................................. 85
  - Upgrading a Data ONTAP cluster nondisruptively by using
    OnCommand System Manager ...................................................... 88
- Upgrading or downgrading Data ONTAP nondisruptively for a two-node
  MetroCluster configuration ............................................................... 89
- Upgrading a Data ONTAP cluster disruptively ...................................... 92
- Completing post-upgrade tasks for cluster upgrades ............................ 94
  - Verifying the cluster version ........................................................... 95
  - Verifying cluster health ................................................................... 96
  - Verifying storage health .................................................................. 97
  - Verifying that IPv6 LIFs can connect to external servers .................. 98
  - Verifying networking and storage status for MetroCluster configurations .................................................. 98
  - Enabling and reverting LIFs to home ports .................................... 101
  - Relocating moved load-sharing mirror source volumes .................. 102
  - Resuming SnapMirror operations ................................................... 102
  - Reenabling automatic LIF rebalancing .......................................... 103
  - Verifying the SAN configuration after an upgrade .......................... 103
Verifying NFS Kerberos configurations after upgrading .................................. 103
Verifying the networking configuration after a major upgrade .................... 104
Enabling volume guarantees after the upgrade .......................................... 105
Configuring LDAP clients to use TLS for highest security ......................... 106
Setting the desired NT ACL permissions display level for NFS clients ....... 107
When you need to update the Disk Qualification Package .......................... 108

Reverting clusters to an earlier Data ONTAP release family .................... 109
When to revert and when to call technical support ....................................... 109
Cluster revert workflow ............................................................................. 110
Planning your reversion ............................................................................ 111
Reviewing pre-reversion resources ........................................................... 110
Reviewing cluster reversion requirements .................................................. 111
Preparing to revert Data ONTAP clusters ................................................. 113
Verifying that the cluster is ready to be reverted ....................................... 113
Preparing to revert production clusters ...................................................... 116
Obtaining Data ONTAP software images ............................................... 122
Installing Data ONTAP software images for a reversion ......................... 122
Reverting a Data ONTAP cluster ............................................................... 124
Completing post-reversion tasks ............................................................... 126
Verifying cluster health ........................................................................... 127
Verifying storage health ........................................................................... 128
Enabling and reverting LIFs to home ports .............................................. 129
Preparing Snapshot copies after reverting .............................................. 131
Verifying client access (CIFS and NFS) ..................................................... 131
Deleting the system SVM for the Cluster IP space .................................. 131
Verifying IPv6 firewall entries .................................................................. 132
Considerations for whether to manually update the SP firmware .............. 133
Considerations for dump backups ............................................................ 133
Creating namespace mirror constituents for reverted Infinite Volumes ...... 133

Downgrading clusters to an earlier release in the same release family ......... 138
When to downgrade and when to call technical support ............................. 138
Cluster downgrade workflow .................................................................... 139
Planning your downgrade ......................................................................... 139
Reviewing pre-downgrade resources ........................................................ 139
Downgrade process considerations .......................................................... 140
Downgrade requirements for MetroCluster configurations ........................ 140
Preparing for the Data ONTAP downgrade process .................................. 141
Verifying that the cluster is ready to be downgraded .................................. 142
Preparing Data ONTAP features for the downgrade .................................. 148
Obtaining Data ONTAP software images ............................................... 152
Performing the software downgrade ......................................................... 152
Downgrading a Data ONTAP cluster nondisruptively ................................ 153
Downgrading a Data ONTAP cluster nondisruptively by using
OnCommand System Manager ................................................................. 156
Upgrading or downgrading Data ONTAP nondisruptively for a two-node MetroCluster configuration ......................................................... 157
Downgrading a Data ONTAP cluster disruptively ......................................................... 160
Completing post-downgrade tasks ........................................................................ 162
Verifying cluster health ....................................................................................... 163
Verifying storage health ...................................................................................... 164
Verifying networking and storage status for MetroCluster configurations .......... 165
Enabling and reverting LIFs to home ports ............................................................ 167
Verifying client access (CIFS and NFS) ............................................................... 168
Resuming SnapMirror operations ........................................................................... 168
Considerations for whether to manually update the SP firmware ....................... 169

Optimal service availability during upgrades .................................................... 170
How upgrades impact service availability ............................................................ 170
Considerations for services and protocols during upgrades ............................... 170
Considerations for stateless protocols .................................................................. 171
Considerations for session-oriented protocols .................................................... 171
How firmware is updated during the Data ONTAP upgrade ................................ 172
Understanding background disk firmware updates .......................................... 172

Upgrading Data ONTAP Edge storage systems ................................................. 174
Upgrade process overview for Data ONTAP Edge storage systems ....................... 174
Recommendations for Data ONTAP Edge systems upgrading to this release ......................... 175
Preparing for a Data ONTAP Edge system upgrade ........................................... 175
Obtaining software images for Data ONTAP Edge systems ............................... 176
Copying the software image to an HTTP or FTP server ...................................... 176
Copying the software image from the HTTP or FTP server to the storage system ................................................................. 176
Software image installation on Data ONTAP Edge systems ............................... 177
Installing software images .................................................................................. 177
Verifying Data ONTAP Edge system status after an upgrade ................................ 178

Copyright information ....................................................................................... 179
Trademark information ....................................................................................... 180
How to send comments about documentation and receive update notifications ................................................................. 181
Index ................................................................................................................... 182
Upgrading Data ONTAP clusters

Upgrading a cluster to the current Data ONTAP release requires planning, 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:

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

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

- Data ONTAP 8.3.x platforms
- Upgrade paths to and within the Data ONTAP 8.3 release family
  The supported upgrade paths include upgrades to releases in the Data ONTAP 8.3 release family from any 8.2.1 or later release (*major upgrades*) and upgrades from 8.3.x to 8.3.z (*minor upgrades*).

**Cluster upgrade workflow**

You can use the cluster upgrade workflow to plan the upgrade, prepare for the upgrade, perform the upgrade, and complete post-upgrade tasks.
Cluster upgrade checklist

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

Steps for planning the upgrade
The planning phase is complete when all of the following steps have been completed:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review pre-upgrade resources. You should review resources to understand</td>
<td></td>
</tr>
<tr>
<td>issues you must resolve before upgrading, understand new system behavior</td>
<td></td>
</tr>
<tr>
<td>in the target release, and confirm hardware support.</td>
<td></td>
</tr>
<tr>
<td>Review the cluster upgrade requirements. There are release and configuration</td>
<td></td>
</tr>
<tr>
<td>requirements that your cluster should meet before you perform an upgrade.</td>
<td></td>
</tr>
<tr>
<td>Additionally, there are mixed version requirements that you should be</td>
<td></td>
</tr>
<tr>
<td>aware of while you are performing the upgrade.</td>
<td></td>
</tr>
<tr>
<td>Condition</td>
<td>Complete?</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>If you have a four-node cluster, understand how epsilon will affect the upgrade sequence. In a four-node cluster, you should plan to upgrade the node that holds epsilon last. This node should always be online to ensure that the cluster can remain in quorum and continue serving data even if one other node unexpectedly goes out of service during the upgrade.</td>
<td></td>
</tr>
<tr>
<td>Understand the estimated duration for the upgrade process. You should plan for at least 30 minutes to complete preparatory steps, 60 minutes to upgrade each HA pair, and at least 30 minutes to complete post-upgrade steps. If you are performing a major NDU, you should plan for at least 30 minutes to install the image on the first node and verify SVM networking.</td>
<td></td>
</tr>
<tr>
<td>Understand the SVM networking requirements. Before upgrading to Data ONTAP 8.3, you should be aware of important networking considerations that affect how SVMs communicate with external services. You should also be prepared to make configuration changes before upgrading to prevent potential disruptions to external servers during the upgrade.</td>
<td></td>
</tr>
<tr>
<td>Understand the requirements for 32-bit data. 32-bit aggregates, volumes, and Snapshot copies are not supported for Data ONTAP 8.3 and later releases. For this reason, you need to understand how the presence of 32-bit data affects the upgrade process and what you can do in advance to minimize the impact.</td>
<td></td>
</tr>
<tr>
<td>Understand the support for root-data partitioning. The Data ONTAP 8.3 release family supports root-data partitioning for entry-level platforms. However, if you upgrade to the Data ONTAP 8.3 release family from a previous release, your system does not support root-data partitioning, even if your platform model supports this feature.</td>
<td></td>
</tr>
<tr>
<td>If you use SnapMirror, understand the upgrade requirements. 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.</td>
<td></td>
</tr>
<tr>
<td>If you have configured an Infinite Volume, understand the upgrade requirements. When upgrading a cluster that is running Data ONTAP 8.2.1 or later and the cluster contains an Infinite Volume, you should upgrade the node with the namespace mirror constituent first and the node with the namespace constituent last to maintain the data protection mirror relationship between constituents.</td>
<td></td>
</tr>
<tr>
<td>If you have a MetroCluster configuration, understand the minor upgrade requirements. Data ONTAP 8.3 supports MetroCluster. If you have a MetroCluster configuration, you can upgrade Data ONTAP nondisruptively within the 8.3 release family. However, you should be aware of some important requirements.</td>
<td></td>
</tr>
</tbody>
</table>
Complete?

<table>
<thead>
<tr>
<th>Condition</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the cluster upgrade limits. Before performing an upgrade, you must verify that your cluster does not exceed the platform system limits. SAN, Hyper-V over SMB, and SQL Server over SMB also have limits that you should verify in addition to the platform system limits.</td>
<td></td>
</tr>
<tr>
<td>If you intend to perform a batch upgrade, plan the upgrade sequence. If you intend to perform a nondisruptive batch upgrade, you should plan the upgrade sequence before you upgrade Data ONTAP. By following the required sequence, you can ensure that the cluster remains up and continues serving data while you perform the NDU.</td>
<td></td>
</tr>
<tr>
<td>Create 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.</td>
<td></td>
</tr>
</tbody>
</table>

**Steps for preparing for a major upgrade**

If you are upgrading from Data ONTAP 8.2, the preparation phase is complete when all of the following steps have been completed:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The HA pair configuration is verified. You can go to the NetApp Support Site and download the Config Advisor tool to check for common configuration errors.</td>
<td></td>
</tr>
<tr>
<td>The HA status is verified. Before performing a nondisruptive upgrade, you should verify that storage failover is enabled for each HA pair. If the cluster consists of only two nodes, you should also verify that cluster HA is enabled.</td>
<td></td>
</tr>
<tr>
<td>The cluster is healthy. You should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.</td>
<td></td>
</tr>
<tr>
<td>The storage is healthy. You should verify the status of your disks, aggregates, and volumes.</td>
<td></td>
</tr>
<tr>
<td>If you are operating in a SAN environment, every volume that contains LUNs must have adequate free space. Before upgrading a cluster in a SAN environment, you must ensure that every volume containing LUNs has available at least 1 MB of free space. The space is needed to accommodate changes in the on-disk data structures used by the new version of Data ONTAP.</td>
<td></td>
</tr>
<tr>
<td>Condition</td>
<td>Complete?</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>All 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.</td>
<td></td>
</tr>
<tr>
<td>LIF failover groups are configured correctly. Before you perform an upgrade, you must verify that the failover policies and failover groups are configured correctly</td>
<td></td>
</tr>
<tr>
<td>If you are operating in a SAN environment, the hosts are configured correctly. Upgrading in a SAN environment changes which paths are direct. Therefore, before performing an upgrade, you should verify that each host is configured with the correct number of direct and indirect paths, and that each host is connected to the correct LIFs.</td>
<td></td>
</tr>
<tr>
<td>The system time is correct. You should verify that NTP is configured, and that the time is synchronized across the cluster.</td>
<td></td>
</tr>
<tr>
<td>No jobs are running. You must verify the status of cluster jobs before upgrading 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.</td>
<td></td>
</tr>
<tr>
<td>Oversized local UNIX user and group names are removed. Beginning with Data ONTAP 8.3, there is a limit of 64 characters for local UNIX user and group names. You can no longer create new user and group names with more than 64 characters, and you must remove existing user and group names with more than 64 characters before upgrading. Name mappings using oversized names will fail after upgrading.</td>
<td></td>
</tr>
<tr>
<td>The netgroup file is present on all nodes. If you have loaded netgroups into SVMs, before you upgrade, you must verify that the netgroup file is present on each node. A missing netgroup file on a node can cause an upgrade to fail.</td>
<td></td>
</tr>
<tr>
<td>File-guaranteed volumes use the correct guarantee type. If your system includes volumes with a guarantee of file that contain space-reserved LUNs or files, and you need the reservations for those LUNs or files to be honored immediately after the upgrade is complete, you should change the space guarantee type of those volumes to volume before you upgrade.</td>
<td></td>
</tr>
<tr>
<td>All non-cluster LIFs use a firewall policy other than cluster. In Data ONTAP 8.3, the cluster firewall policy blocks access to most management services, such as SSH and DNS. Therefore, before performing a major upgrade, you should ensure that all non-cluster LIFs use a firewall policy other than cluster.</td>
<td></td>
</tr>
</tbody>
</table>
### Condition

<table>
<thead>
<tr>
<th>Complete?</th>
</tr>
</thead>
</table>
| **All LIFs are enabled and located on their home ports.**
  
  During a reboot, some LIFs might have been migrated to their assigned failover ports. Before you upgrade, you must enable and revert any LIFs that are not on their home ports. |

| **The SVM networking is configured to reach all external servers.**
  
  Before performing a major upgrade from Data ONTAP 8.2, you must configure a data LIF for each data SVM that can reach all external servers. You must also ensure that failover groups and routes are configured to enable these LIFs to reach all external servers throughout the upgrade. |

| **All FlexCache volumes are removed.**
  
  Before upgrading to Data ONTAP 8.3, you must identify and remove any FlexCache volumes. |

| **Any active CIFS sessions that should be terminated have been identified.**
  
  Before performing a nondisruptive upgrade, you should identify and gracefully terminate any CIFS sessions that are not continuously available. |

| **All load-sharing mirror source volumes are located on the last node to be upgraded.**
  
  Before performing a major upgrade from Data ONTAP 8.2, you should move all of the load-sharing mirror source volumes to an aggregate on the node that you will upgrade last. This ensures that load-sharing mirror destination volumes are the same or later versions of Data ONTAP. |

| **All SnapMirror operations are suspended.**
  
  You must suspend SnapMirror operations before performing a nondisruptive upgrade of Data ONTAP. |

| **The target Data ONTAP software image is obtained.**
  
  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. |

| **The target Data ONTAP software image is installed on each node.**
  
  Before performing a major upgrade to Data ONTAP 8.3, you must install the software image on the first node to verify that each SVM will be able to reach its external servers during the upgrade. After the image installation succeeds, you install the software image on the remaining nodes. |

| **The 32-bit capability is disabled.**
  
  Before you can upgrade your cluster to Data ONTAP 8.3, you must remove all 32-bit data and disable the 32-bit capability. You must complete this task even if you have never created 32-bit aggregates on your cluster. |

### Steps for preparing for a minor upgrade

If you are upgrading within the Data ONTAP 8.3 release family, the preparation phase is complete when all of the following steps have been completed:
<table>
<thead>
<tr>
<th>Condition</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The HA pair or MetroCluster configuration is verified.</td>
<td></td>
</tr>
<tr>
<td>You can go to the NetApp Support Site and download the Config Advisor</td>
<td></td>
</tr>
<tr>
<td>tool to check for common configuration errors.</td>
<td></td>
</tr>
<tr>
<td>The HA status is verified.</td>
<td></td>
</tr>
<tr>
<td>Before performing a nondisruptive upgrade, you should verify that</td>
<td></td>
</tr>
<tr>
<td>storage failover is enabled for each HA pair. If the cluster consists</td>
<td></td>
</tr>
<tr>
<td>of only two nodes, you should also verify that cluster HA is enabled.</td>
<td></td>
</tr>
<tr>
<td>The cluster is healthy.</td>
<td></td>
</tr>
<tr>
<td>You should verify that the nodes are healthy and eligible to</td>
<td></td>
</tr>
<tr>
<td>participate in the cluster, and that the cluster is in quorum.</td>
<td></td>
</tr>
<tr>
<td>The storage is healthy.</td>
<td></td>
</tr>
<tr>
<td>You should verify the status of your disks, aggregates, and volumes.</td>
<td></td>
</tr>
<tr>
<td>If you are operating in a SAN environment, every volume that contains</td>
<td></td>
</tr>
<tr>
<td>LUNs must have adequate free space.</td>
<td></td>
</tr>
<tr>
<td>Before upgrading a cluster in a SAN environment, you must ensure that</td>
<td></td>
</tr>
<tr>
<td>every volume containing LUNs has available at least 1 MB of free space.</td>
<td></td>
</tr>
<tr>
<td>The space is needed to accommodate changes in the on-disk data structures</td>
<td></td>
</tr>
<tr>
<td>used by the new version of Data ONTAP.</td>
<td></td>
</tr>
<tr>
<td>If you have a MetroCluster configuration, the networking and storage</td>
<td></td>
</tr>
<tr>
<td>status is healthy and in the correct state.</td>
<td></td>
</tr>
<tr>
<td>You should verify the status of the LIFs, aggregates, and volumes for</td>
<td></td>
</tr>
<tr>
<td>each cluster.</td>
<td></td>
</tr>
<tr>
<td>All deduplicated volumes and aggregates contain sufficient free space.</td>
<td></td>
</tr>
<tr>
<td>Before upgrading Data ONTAP, you must verify that any deduplicated</td>
<td></td>
</tr>
<tr>
<td>volumes and the aggregates that contain them have sufficient free space</td>
<td></td>
</tr>
<tr>
<td>for the deduplication metadata. If there is insufficient free space,</td>
<td></td>
</tr>
<tr>
<td>deduplication will be disabled when the Data ONTAP upgrade is completed.</td>
<td></td>
</tr>
<tr>
<td>LIF failover groups are configured correctly.</td>
<td></td>
</tr>
<tr>
<td>Before you perform an upgrade, you must verify that the failover</td>
<td></td>
</tr>
<tr>
<td>policies and failover groups are configured correctly</td>
<td></td>
</tr>
<tr>
<td>If you are operating in a SAN environment, the hosts are configured</td>
<td></td>
</tr>
<tr>
<td>correctly.</td>
<td></td>
</tr>
<tr>
<td>Upgrading in a SAN environment changes which paths are direct. Therefore,</td>
<td></td>
</tr>
<tr>
<td>before performing an upgrade, you should verify that each host is</td>
<td></td>
</tr>
<tr>
<td>configured with the correct number of direct and indirect paths, and</td>
<td></td>
</tr>
<tr>
<td>that each host is connected to the correct LIFs.</td>
<td></td>
</tr>
<tr>
<td>The system time is correct.</td>
<td></td>
</tr>
<tr>
<td>You should verify that NTP is configured, and that the time is</td>
<td></td>
</tr>
<tr>
<td>synchronized across the cluster.</td>
<td></td>
</tr>
</tbody>
</table>
### Condition | Complete?
--- | ---
No jobs are running. You must verify the status of cluster jobs before upgrading 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. |  
All LIFs are enabled and located on their home ports. During a reboot, some LIFs might have been migrated to their assigned failover ports. Before you upgrade, you must enable and revert any LIFs that are not on their home ports. |  
If you are performing a batch upgrade, automatic LIF rebalancing must be disabled. By disabling automatic LIF rebalancing before performing a batch upgrade, you can ensure that the LIFs remain online during the entire upgrade procedure. |  
Any active CIFS sessions that should be terminated have been identified. Before performing a nondisruptive upgrade, you should identify and gracefully terminate any CIFS sessions that are not continuously available. |  
All SnapMirror operations are suspended. You must suspend SnapMirror operations before performing a nondisruptive upgrade of Data ONTAP. |  
The target Data ONTAP software image is obtained. 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. |  
The target Data ONTAP software image is installed on each node. Before performing a major upgrade to Data ONTAP 8.3, you must install the software image on the first node to verify that each SVM will be able to reach its external servers during the upgrade. After the image installation succeeds, you install the software image on the remaining nodes. |  

**Steps for performing a rolling upgrade (major or minor NDU)**

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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The first HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded.</td>
</tr>
<tr>
<td></td>
<td>The node’s partner is upgraded.</td>
</tr>
<tr>
<td>If needed, the second HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded.</td>
</tr>
<tr>
<td></td>
<td>The node’s partner is upgraded.</td>
</tr>
<tr>
<td>Condition</td>
<td>Complete?</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
</tr>
<tr>
<td>If needed, the third HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded. The node's partner is upgraded.</td>
</tr>
<tr>
<td>If needed, the fourth HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded. The node's partner is upgraded.</td>
</tr>
<tr>
<td>If needed, the fifth HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded. The node's partner is upgraded.</td>
</tr>
<tr>
<td>If needed, the sixth HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded. The node's partner is upgraded.</td>
</tr>
<tr>
<td>If needed, the seventh HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded. The node's partner is upgraded.</td>
</tr>
<tr>
<td>If needed, the eighth HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded. The node's partner is upgraded.</td>
</tr>
<tr>
<td>If needed, the ninth HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded. The node's partner is upgraded.</td>
</tr>
<tr>
<td>If needed, the tenth HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded. The node's partner is upgraded.</td>
</tr>
<tr>
<td>If needed, the eleventh HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded. The node's partner is upgraded.</td>
</tr>
<tr>
<td>If needed, the twelfth HA pair is upgraded.</td>
<td>The first node in the HA pair is upgraded. The node's partner is upgraded.</td>
</tr>
</tbody>
</table>

**Steps for performing a batch upgrade (minor NDU only)**
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:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
The first batch is upgraded.
The first node in each HA pair is upgraded.
The nodes’ partners are upgraded.

The second batch is upgraded.
The first node in each HA pair is upgraded.
The nodes’ partners are upgraded.

Steps for after performing a major upgrade
The post-upgrade phase is complete when all of the following steps have been completed:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The cluster version is correct. After all of the HA pairs have been upgraded, you must use the <code>version</code> command to verify that all of the nodes are running the target release.</td>
<td></td>
</tr>
<tr>
<td>The cluster is healthy. You should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.</td>
<td></td>
</tr>
<tr>
<td>The storage is healthy. You should verify the status of your disks, aggregates, and volumes.</td>
<td></td>
</tr>
<tr>
<td>Any IPv6 SVM management LIFs can connect to external servers. Data ONTAP 8.2.2 and earlier can only verify that each SVM can connect to its external servers through IPv4 addresses. Therefore, after upgrading to Data ONTAP 8.3, you should verify that each SVM can connect to an external server using an IPv6 address.</td>
<td></td>
</tr>
<tr>
<td>All LIFs are enabled and located on their home ports. During a reboot, some LIFs might have been migrated to their assigned failover ports. After you upgrade, you must enable and revert any LIFs that are not on their home ports.</td>
<td></td>
</tr>
<tr>
<td>All load-sharing mirror source volumes are relocated to the correct nodes. After successfully completing a nondisruptive upgrade, you can move load-sharing mirror source volumes back to the locations they were in originally before the upgrade.</td>
<td></td>
</tr>
<tr>
<td>SnapMirror operations are resumed. After completing a nondisruptive upgrade, you must resume any SnapMirror relationships that were suspended.</td>
<td></td>
</tr>
<tr>
<td>If you are operating in a SAN environment, all hosts have reconnected to their LIFs. If you are upgrading in a SAN environment, then after the upgrade, you should verify that each initiator that was connected to a LIF before the upgrade has successfully reconnected to the LIF.</td>
<td></td>
</tr>
</tbody>
</table>
The Kerberos configuration is verified.
Beginning with Data ONTAP 8.3, Data ONTAP restricts the use of identical service principal names (SPNs) for NFS Kerberos configurations when used across multiple SVMs and deletes NFS Kerberos configurations that are no longer permitted. To avoid NFS client Kerberos authentication problems after upgrading, you must check whether your system is affected by this change and reconfigure accordingly.

The networking configuration is verified.
After completing a major upgrade to Data ONTAP 8.3, you should verify that the SVM management LIFs, failover groups, and broadcast domains are configured correctly for your environment.

If necessary, volume guarantees are enabled.
If your cluster included FlexVol volumes with a guarantee of file before the upgrade, and those volumes contained space-reserved LUNs or files, the volumes have a disabled guarantee after the upgrade. To provide the same guarantee to those files and LUNs, you must enable the guarantee for those volumes.

LDAP clients are configured to use TLS for highest security.
If you had previously configured LDAP clients to use LDAP over SSL/TLS for secure communications with LDAP servers, the LDAP client was able to use the less secure SSLv2 protocol. After upgrading to this release, if your environment supports it, you should disallow the use of SSLv2 to force the use of TLS for the highest level of security.

If necessary, the Disk Qualification Package (DQP) is updated.
The 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.

---

**Steps for after performing a minor upgrade**
The post-upgrade phase is complete when all of the following steps have been completed:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The cluster version is correct. After all of the HA pairs have been upgraded, you must use the <code>version</code> command to verify that all of the nodes are running the target release.</td>
<td></td>
</tr>
<tr>
<td>The cluster is healthy. You should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.</td>
<td></td>
</tr>
<tr>
<td>The storage is healthy. You should verify the status of your disks, aggregates, and volumes.</td>
<td></td>
</tr>
<tr>
<td>If you have a MetroCluster configuration, the networking and storage status is healthy and in the correct state. You should verify the status of the LIFs, aggregates, and volumes for each cluster.</td>
<td></td>
</tr>
</tbody>
</table>
## Condition

<table>
<thead>
<tr>
<th>Condition</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>All LIFs are enabled and located on their home ports.</td>
<td></td>
</tr>
<tr>
<td>During a reboot, some LIFs might have been migrated to their assigned</td>
<td></td>
</tr>
<tr>
<td>failover ports. After you upgrade, you must enable and revert any LIFs</td>
<td></td>
</tr>
<tr>
<td>that are not on their home ports.</td>
<td></td>
</tr>
<tr>
<td>SnapMirror operations are resumed.</td>
<td></td>
</tr>
<tr>
<td>After completing a nondisruptive upgrade, you must resume any SnapMirror</td>
<td></td>
</tr>
<tr>
<td>relationships that were suspended.</td>
<td></td>
</tr>
<tr>
<td>LIF rebalancing is reenabled if it was previously disabled.</td>
<td></td>
</tr>
<tr>
<td>If you previously disabled automatic LIF rebalancing to perform a batch</td>
<td></td>
</tr>
<tr>
<td>upgrade, you should reenable it after completing the upgrade.</td>
<td></td>
</tr>
<tr>
<td>If you are operating in a SAN environment, all hosts have reconnected to</td>
<td></td>
</tr>
<tr>
<td>their LIFs.</td>
<td></td>
</tr>
<tr>
<td>If you are upgrading in a SAN environment, then after the upgrade, you</td>
<td></td>
</tr>
<tr>
<td>should verify that each initiator that was connected to a LIF before the</td>
<td></td>
</tr>
<tr>
<td>upgrade has successfully reconnected to the LIF.</td>
<td></td>
</tr>
<tr>
<td>If necessary, the Disk Qualification Package (DQP) is updated.</td>
<td></td>
</tr>
<tr>
<td>The DQP adds full support for newly qualified drives. Before you update</td>
<td></td>
</tr>
<tr>
<td>drive firmware or add new drive types or sizes to a cluster, you must</td>
<td></td>
</tr>
<tr>
<td>update the DQP. A best practice is to also update the DQP regularly; for</td>
<td></td>
</tr>
<tr>
<td>example, every quarter or semi-annually.</td>
<td></td>
</tr>
</tbody>
</table>

## 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.

### Nondisruptive upgrades

In a *nondisruptive upgrade* (NDU), the cluster remains online and continues to serve data during the upgrade. The following table describes the three NDU methods:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Release requirements</th>
<th>Cluster size requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rolling upgrade</td>
<td>A node is taken offline and upgraded while its partner takes over its storage. When the node upgrade is complete, the partner node gives control back to the original owning node and the process is repeated, this time on the partner node. Each additional HA pair is upgraded in sequence until all HA pairs are running the target release.</td>
<td>This method is required for major NDUs.</td>
<td>The cluster must consist of two or more nodes.</td>
</tr>
</tbody>
</table>
### Batch upgrade

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 partner nodes take over their storage. When the upgrade is completed for the first half of all of the HA pairs, the partner nodes give control back to the original owning nodes, and the process is repeated, this time on the partner nodes. The process is then repeated on the second batch.

**Release requirements:** Minor NDU only.
**Cluster size requirements:** The cluster must consist of eight or more nodes.

### Automated upgrade

Data ONTAP automatically installs the target Data ONTAP image on each node, validates the cluster components to ensure that the cluster can be upgraded nondisruptively, and then, based on the number of nodes in the cluster, executes either a rolling or batch upgrade in the background.

**Release requirements:** Minor NDU only. This method is recommended for all upgrades within the Data ONTAP 8.3 release family.
**Cluster size requirements:** The cluster must consist of two or more nodes.

### Disruptive upgrades

In a *disruptive upgrade*, storage failover is disabled for each HA pair, and then each node is rebooted one at a time. Disruptive upgrades can be performed more quickly than nondisruptive upgrades, and require fewer steps to complete. However, you should not perform a disruptive upgrade unless you can take the cluster offline for the duration of the upgrade. If you are operating in a SAN environment, you should be prepared to shut down or suspend all SAN clients before performing a disruptive upgrade.

If the cluster is a single-node cluster, you can upgrade it only by performing a disruptive upgrade.

**Related tasks**

- Planning the upgrade sequence for a batch upgrade on page 29
- Planning an upgrade to a Data ONTAP Edge storage system

### Planning an upgrade to a Data ONTAP Edge storage system

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 Edge storage systems and to the *Data ONTAP-v Administration Tool Installation Guide*.

**Related concepts**

- Upgrading Data ONTAP Edge storage systems on page 174
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:
   ```bash
   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.
   ```text
   NetApp AutoSupport
   ```

3. Click the Launch My AutoSupport link.

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 Upgrade To menu.

9. Select the upgrade method and the level of detail you want included in your upgrade plan.
10. Click Generate 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.

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.

Unless otherwise indicated, the requirements and procedures in this guide apply to all supported Data ONTAP 8.3.x platforms.

Steps

1. Reviewing pre-upgrade resources on page 21
   Before upgrading Data ONTAP, you should review resources to understand issues you must resolve before upgrading, understand new system behavior in the target release, and confirm hardware support.

2. Reviewing cluster upgrade requirements on page 21
   Before upgrading Data ONTAP, you must verify that your cluster meets the general upgrade requirements. Some configurations and features also have requirements that you should understand.

3. Verifying cluster upgrade limits on page 28
   Before performing an upgrade, you must verify that your cluster does not exceed the platform system limits. SAN, Hyper-V over SMB, and SQL Server over SMB also have limits that you should verify in addition to the platform system limits.

4. Planning the upgrade sequence for a batch upgrade on page 29
   If you intend to perform a nondisruptive batch upgrade, you should plan the upgrade sequence before you upgrade Data ONTAP. By following the required sequence, you can ensure that the cluster remains up and continues serving data while you perform the NDU.

5. Creating a performance baseline with Perfstat Converged on page 30
   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.

Related concepts

Downgrading clusters to an earlier release in the same release family on page 138
Reverting clusters to an earlier Data ONTAP release family on page 109
Reviewing pre-upgrade resources

Before upgrading Data ONTAP, you should review resources to understand issues you must resolve before upgrading, understand new system behavior in the target release, and confirm hardware support.

Steps

   
   *Find the Release Notes for your version of Data ONTAP 8*
   
   The “Important cautions” section describes potential issues that you should be aware of before upgrading to the new release. The “New and changed features” and “Known problems and limitations” sections describe new system behavior after upgrading to the new release.

2. Confirm that your hardware platform is supported in the target release.
   
   *NetApp Hardware Universe*

3. Confirm that your cluster and management switches are supported in the target release.
   
   You must verify that the NX-OS (cluster network switches), IOS (management network switches), and reference configuration file (RCF) software versions are compatible with the version of Data ONTAP to which you are upgrading. If your switches do not have the minimum software versions for the target Data ONTAP release, then you must upgrade the switch software before you can upgrade Data ONTAP.
   
   *NetApp Downloads: Cisco Ethernet Swtich*

4. If your cluster is configured for SAN, confirm that the SAN configuration is fully supported.
   
   All SAN components—including the target Data ONTAP software version, host OS and patches, required Host Utilities software, and adapter drivers and firmware—should be supported.
   
   *NetApp Interoperability Matrix Tool*

5. If you are transitioning from 7-Mode using the 7-Mode Transition Tool, confirm that the tool supports transition to the clustered Data ONTAP version to which you are upgrading.
   
   All the projects in the tool must be in the completed or aborted state before you upgrade the 7-Mode Transition Tool that supports the clustered Data ONTAP version to which you are upgrading.
   
   *7-Mode Transition Tool 2.2 Installation and Setup Guide*

Reviewing cluster upgrade requirements

Before upgrading Data ONTAP, you must verify that your cluster meets the general upgrade requirements. Some configurations and features also have requirements that you should understand.

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 8.3 release family from any 8.2.1 or later release. Minor upgrades within the Data ONTAP 8.3 release family are supported from all previous 8.3 releases. You can determine the current version of Data ONTAP running on each node by using the system image show command.
Note: If you are running Data ONTAP GX 10.x, do not attempt to upgrade clusters to the Data ONTAP 8.3 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 8.3 release from a release earlier than 8.2.1, you must perform an intermediate upgrade (also known as a multi-hop upgrade) to Data ONTAP 8.2.1 or later before upgrading to the target Data ONTAP 8.3 release.

Find the Upgrade and Revert/Downgrade Guide for your version of Data ONTAP 8

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.
  
  *Clustered Data ONTAP 8.3 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 and SQL Server over SMB solutions.
  These solutions enable the application servers and the contained virtual machines or databases to stay online and to provide continuous availability during the Data ONTAP upgrade.
  
  *Clustered Data ONTAP 8.3 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.

- If the cluster serves SAN clients, you can use the batch upgrade method only if you are upgrading within the Data ONTAP 8.3 release family.
  If you are upgrading from Data ONTAP 8.2, do not use the batch upgrade method. You should perform a rolling upgrade instead.

- 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. You should complete the upgrade as quickly as possible; do not allow the cluster to remain in a mixed version state longer than necessary.

How epsilon affects the upgrade sequence for four-node clusters

In a four-node cluster, you should plan to upgrade the node that holds epsilon last. This node should always be online to ensure that the cluster can remain in quorum and continue serving data even if one other node unexpectedly goes out of service during the upgrade.

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.

Related information

Clustered Data ONTAP 8.3 System Administration Guide

Guidelines for estimating the duration of the upgrade process

You should plan for at least 30 minutes to complete preparatory steps, 60 minutes to upgrade each HA pair, and at least 30 minutes to complete post-upgrade steps. If you are performing a major NDU, you should plan for at least 30 minutes to install the image on the first node and verify SVM networking.

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. However, the actual duration of your upgrade process will depend on your individual environment.

SVM networking considerations for major upgrades

Before upgrading to Data ONTAP 8.3, you should be aware of important networking considerations that affect how Storage Virtual Machines (SVMs) communicate with external services. You should also be prepared to make configuration changes before upgrading to prevent potential disruptions to external servers during the upgrade.

Starting in Data ONTAP 8.3, an SVM can only communicate with the following external services by using one of its own LIFs:

- DNS, NIS, and LDAP servers
- Active Directory servers
- Kerberos servers
- Domain Controllers
- iSNS server
- Policy server (if you are using FPolicy)

After you upgrade a node to Data ONTAP 8.3, SVMs can no longer initiate connections to external servers through the node's node management LIF. Instead, each SVM must use one of its own LIFs, which must be hosted on a node running the 8.3 release.

As part of the upgrade preparation, you should be prepared to configure your network so that it meets the following requirements:

- Each SVM must be able to reach each of its external servers through a data LIF.

As part of the upgrade preparation, you either configure existing data LIFs or create SVM management LIFs (dedicated LIFs with no data protocol configured) that can reach each external server. You also ensure that failover groups and routes are configured to enable these LIFs to reach all external servers throughout the upgrade.

Note: If you plan to create any SVM management LIFs, you must have a permanent IP address available for each LIF.
• If a firewall is configured between the cluster and the external servers:
  ◦ The firewall must accept ICMP packets from the data LIFs that you configured for external server connectivity.
    When you install the Data ONTAP 8.3 image on the first node, Data ONTAP attempts to ping each external server using ICMP packets to verify the networking configuration. If the firewall filters out the ICMP packets, the image installation will fail. To resolve this issue, you can open the firewall to accept ICMP packets for the IP addresses of the data LIFs that you configured for external server connectivity. You can close the firewall after the upgrade is complete.
  ◦ The firewall must allow all data LIFs to reach external servers using their TCP/UDP service ports.

• The data LIFs that each SVM uses to connect to external servers must be located on the first node to be upgraded.
  After the first node is upgraded and running Data ONTAP 8.3, SVMs can no longer initiate connections to external servers through the node's node management LIF. Therefore, by placing the data LIFs that are configured to connect to external servers on the first node, you ensure that all SVMs can reach their external servers throughout the upgrade.

• The second node to be upgraded must be capable of hosting all of the first node's SVM management LIFs.

• The first node to be upgraded must not exceed 128 data LIFs.
  If your cluster contains a large number of SVMs or LIFs, the first node might not be able to host its own data LIFs in addition to the SVM LIFs used to communicate with external servers.

• If you are upgrading from Data ONTAP 8.2.2 or earlier, the cluster must not use IPv6 addresses to reach external services.
  If you upgrade from Data ONTAP 8.2.2 or earlier, Data ONTAP cannot verify that external servers are reachable from IPv6 addresses before the upgrade (although you can verify connectivity after the upgrade is complete by using the `vserver check lif-multitenancy run` command).

• If you are upgrading from Data ONTAP 8.2.1, the cluster must not have separate management and data networks.
  If the external servers are only accessible from node management LIFs, a nondisruptive upgrade is only possible if you do one of the following:
  ◦ Upgrade to Data ONTAP 8.2.2 GA or later so that you can configure the data LIFs needed for external connectivity on node management ports.
  ◦ Wire a data port from each node in the first HA pair to a network that can reach the external servers.

Related tasks

Prepating SVM networking for a major upgrade on page 47
Installing Data ONTAP software images for a major upgrade on page 56

Before performing a major upgrade to Data ONTAP 8.3, you must install the software image on the first node to verify that each SVM will be able to reach its external servers during the upgrade. After the image installation succeeds, you install the software image on the remaining nodes.
Upgrade considerations regarding 32-bit data

32-bit aggregates, volumes and Snapshot copies are not supported for Data ONTAP 8.3 and later releases. For this reason, you need to understand how the presence of 32-bit data affects the upgrade process and what you can do in advance to minimize the impact.

32-bit data can be present even if you have expanded all of your aggregates to the 64-bit format, and it could take several weeks or more to remove all of it, depending on the method you use.

You disable the 32-bit capability as part of upgrade preparation. This step cannot be completed unless all 32-bit data has been removed, and cannot be done in advance. However, to ensure that you can disable the 32-bit capability quickly and easily later, you can check for and remove any 32-bit data that you find now. The `storage aggregate 64bit-upgrade 32bit-disable` command with the `-check` parameter enables you to determine which aggregates have 32-bit data without actually disabling the capability.

**Attention:** You cannot disable the 32-bit capability now.

Related tasks

*Disabling the 32-bit capability* on page 59

Before you can upgrade your cluster to Data ONTAP 8.3, you must remove all 32-bit data and disable the 32-bit capability. You must complete this task even if you have never created 32-bit aggregates on your cluster.

Upgrade considerations for root-data partitioning

Starting with Data ONTAP 8.3, root-data partitioning is supported for some platform models and configurations. The root-data partitioning capability is enabled during system initialization; it cannot be applied to existing aggregates. When a node is upgraded to Data ONTAP 8.3 from a previous release, the root aggregate remains configured on unpartitioned disks.

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

Related information

*Clustered Data ONTAP 8.3 Physical Storage Management Guide*

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

<table>
<thead>
<tr>
<th>Description</th>
<th>Upgrade destination nodes before source nodes?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspend SnapMirror operations for the duration of the NDU (nondisruptive upgrade).</td>
<td>No, the nodes can be upgraded in any order.</td>
</tr>
<tr>
<td>Suspend SnapMirror operations one destination volume at a time.</td>
<td>Yes.</td>
</tr>
</tbody>
</table>

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.

**Related information**

*Clustered Data ONTAP 8.3 Data Protection Guide*

**Upgrade considerations for an Infinite Volume**

When upgrading a cluster that is running Data ONTAP 8.2.1 or later, and the cluster contains an Infinite Volume, you should upgrade the node with the namespace mirror constituent first and the node with the namespace constituent last to maintain the data protection mirror relationship between constituents.

For an Infinite Volume with SnapDiff enabled to support incremental tape backup, each node with a data constituent also includes either the namespace constituent or a namespace mirror constituent. In this case, you should upgrade all nodes with a namespace mirror constituent before you upgrade the node with the namespace constituent. Incremental tape backup and restore operations are unavailable until you finish upgrading all nodes that the Infinite Volume spans.

If you upgrade the node with the namespace constituent before you upgrade the node or nodes with the namespace mirror constituents, the data protection mirror relationship will not be updated until all nodes in the cluster are upgraded. As a result, the namespace mirror constituent is not updated until all nodes in the cluster are upgraded.
**Note:** The recommended order for upgrading nodes applies only when upgrading a cluster that contains an Infinite Volume from Data ONTAP 8.2.1 or later to Data ONTAP 8.3.0. When upgrading a cluster that contains an Infinite Volume from Data ONTAP 8.3.0 to Data ONTAP 8.3.x, you can upgrade the nodes in any order.

After the upgrade, you might notice dongle files in the namespace constituent. The dongle files are harmless, and you can choose whether to leave the dongle files in the namespace constituent or delete the dongle files.

### Upgrade requirements for MetroCluster configurations

Data ONTAP 8.3 supports MetroCluster configurations. If you have a MetroCluster configuration, you can upgrade Data ONTAP nondisruptively within the 8.3 release family. However, you should be aware of some important requirements.

#### General requirements

- Both clusters must be running the same version of Data ONTAP. You can verify the Data ONTAP version by using the `version` command.
- The MetroCluster configuration must be in either normal or switchover mode.
- You can upgrade both clusters at the same time, or upgrade one cluster before the other. The upgrade is nondisruptive regardless of which cluster you upgrade first.
- The aggregates in both clusters must not be in resyncing RAID status. During MetroCluster healing, the mirrored aggregates are resynchronized. You can verify whether the MetroCluster configuration is in this state by using the `storage aggregate plex show -in-progress true` command. If any aggregates are in progress, you should not perform an upgrade until the aggregate resynchronization is complete.
- Negotiated switchover operations will fail while the upgrade is in progress. After the upgrade has started, you should not attempt a negotiated switchover until both clusters have been upgraded and all nodes are running the same version of Data ONTAP. If a site failure occurs during the upgrade, you should perform a forced switchover.

#### Configuration requirements for normal operation

- The source SVM LIFs must be up and located on their home nodes. Data LIFs for the destination SVMs are not required to be up or to be on their home nodes.
- All aggregates at the local site must be online.
- All root and data volumes owned by the local cluster's SVMs must be online.

#### Configuration requirements for switchover

- All LIFs must be up and located on their home nodes.
- All aggregates must be online, except for the root aggregates at the DR site. Root aggregates at the DR site are offline during certain phases of switchover.
- All volumes must be online.

### Related tasks

[Verifying networking and storage status for MetroCluster configurations](page 36)
Upgrade requirement for netgroups

If you use netgroups in export policy rules for client matching, you must be aware of a DNS configuration requirement to ensure that your export policies continue to properly match clients after upgrading.

Data ONTAP performs a reverse DNS lookup on the IP address of clients to compare against the host names contained in a netgroup when matching clients with export policy rules containing a netgroup. The reverse DNS lookup and the resulting host name comparison must succeed for Data ONTAP to properly match clients.

For this reason, if you use netgroups in export policy rules and your netgroups contain host names, all host names in netgroups must have both forward (A) and reverse (PTR) DNS records to ensure consistent forward and reverse DNS lookups.

In addition, if an IP address of a client has multiple PTR records, all those host names must be members of the netgroup and have corresponding A records.

Verifying cluster upgrade limits

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

Steps

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

   *NetApp Hardware Universe*

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

   *Clustered Data ONTAP 8.3 SAN Configuration Guide*

3. Verify the following limits for each node:
   a. Determine the CPU and disk utilization:
      
      ```
      node run -node node_name -command sysstat -c 10 -x 3
      ```
      
      You should monitor CPU and disk utilization for 30 seconds. The values in the CPU and Disk Util columns should not exceed 50% for all 10 measurements reported. No additional load should be added to the cluster until the upgrade is complete.
   b. Optional: If the cluster is configured for Hyper-V or SQL Server over SMB, determine the number of volumes hosted by the node:
      
      ```
      volume show -node node_name
      ```
      
      The node must not host more than 200 volumes.
   c. Optional: If the cluster is configured for both SAN and Hyper-V or SQL Server over SMB, determine the number of LUNs hosted by the node:
      
      ```
      lun show -node node_name
      ```
      
      The node must not host more than 400 LUNs.
Planning the upgrade sequence for a batch upgrade

If you intend to perform a nondisruptive batch upgrade, you should plan the upgrade sequence before you upgrade Data ONTAP. By following the required sequence, you can ensure that the cluster remains up and continues serving data while you perform the NDU.

About this task

Batch upgrades are only supported for minor upgrades within the Data ONTAP 8.3 release family. If you are upgrading from Data ONTAP 8.2, you must perform a rolling upgrade.

Steps

1. Divide the cluster into two batches:

<table>
<thead>
<tr>
<th>If the cluster contains an...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Even number of HA pairs</td>
<td>Place half of the HA pairs in the first batch, and the other half of the HA pairs in the second batch.</td>
</tr>
<tr>
<td>Odd number of HA pairs</td>
<td>Place the larger number of HA pairs in the first batch, and the smaller number of HA pairs in the second batch.</td>
</tr>
</tbody>
</table>

Example

In this example, the cluster contains six HA pairs. Three HA pairs are placed in each batch.

Example

In this example, the cluster contains seven HA pairs. Four HA pairs are placed in the first batch, and three HA pairs are placed in the second batch.

2. Determine the upgrade sequence for each batch.

   In a batch, a node from each HA pair is upgraded concurrently while their respective partners take over their storage. Then the partners are upgraded concurrently while the original nodes take over their storage.

Example

In this 12-node cluster, the nodes would be upgraded in the following sequence:
In the first batch, upgrade nodes A, C, and E concurrently.

In the first batch, upgrade nodes B, D, and F concurrently.

In the second batch, upgrade nodes G, I, and K concurrently.

In the second batch, upgrade nodes H, J, and L concurrently.

Example

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

In the first batch, upgrade nodes A, C, E, and G concurrently.

In the first batch, upgrade nodes B, D, F, and H concurrently.

In the second batch, upgrade nodes I, K, and M concurrently.

In the second batch, upgrade nodes J, L, and N concurrently.

Related concepts

Types of cluster upgrades on page 17

Related tasks

Upgrading a Data ONTAP cluster nondisruptively by using the batch method on page 73

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.

Clustered Data ONTAP 8.3 System Administration Guide
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.
   
   NetApp Downloads: Performance and Statistics Collector (Perfstat)

2. Enter the following command during a typical usage period:
   
   \texttt{perfstat8 \textit{cluster\_management\_IP\_address} \textit{-m c \textit{-t 4 \textit{-i 5 \textit{-z}}}}

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

Preparing for a Data ONTAP cluster upgrade
Before performing an upgrade, you must verify that the cluster is ready to be upgraded, make any required configuration changes, obtain and install the target Data ONTAP images, and if necessary, disable the 32-bit capability.

Steps
1. Verifying that the cluster is ready to be upgraded on page 31
   Before you perform the upgrade, you should verify that your cluster configuration is healthy.

2. Preparing Data ONTAP features for the upgrade on page 43
   Some Data ONTAP features have configuration requirements that must be completed before the cluster can be upgraded.

3. Obtaining Data ONTAP software images on page 55
   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.

4. Installing Data ONTAP software images for a major upgrade on page 56
   Before performing a major upgrade to Data ONTAP 8.3, you must install the software image on the first node to verify that each SVM will be able to reach its external servers during the upgrade. After the image installation succeeds, you install the software image on the remaining nodes.

5. Disabling the 32-bit capability on page 59
   Before you can upgrade your cluster to Data ONTAP 8.3, you must remove all 32-bit data and disable the 32-bit capability. You must complete this task even if you have never created 32-bit aggregates on your cluster.

Verifying that the cluster is ready to be upgraded
Before you perform the upgrade, you should verify that your cluster configuration is healthy.

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 [mysupport.netapp.com](https://mysupport.netapp.com) and go to Downloads > Software > ToolChest.
2. Click Config Advisor.
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 provided to address any issues discovered.

**Checking for MetroCluster configuration errors with Config Advisor**

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. You can deploy it 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. Go to NetApp Downloads: Config Advisor.
2. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

**Verifying HA status**

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

**About this task**

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

**Steps**

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

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

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

   ```bash
   cluster ha show
   ``

   **Example**

   This example shows that cluster HA is configured:

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

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

### Verifying cluster 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 that the cluster is in quorum.

#### Steps

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

   ```bash
   cluster show
   ``

   **Example**

   ```bash
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node0                 true    true
   node1                 true    true
   ``

   If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:

   ```bash
   set -privilege advanced
   ``

   Enter `y` to continue.

3. Verify the configuration details for each RDB process.

   You should verify the following configuration details:
   
   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.
     
     Note that each ring might have a different quorum master.

     **To display this RDB process...**  **Enter this command...**
     
     Management application  `cluster ring show -unitname mgmt`
     
     Volume location database  `cluster ring show -unitname 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:

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

<table>
<thead>
<tr>
<th>Node</th>
<th>UnitName</th>
<th>Epoch</th>
<th>DB Epoch</th>
<th>DB Trxns</th>
<th>Master</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>vldb</td>
<td>154</td>
<td>154</td>
<td>14847</td>
<td>node0</td>
<td>master</td>
</tr>
<tr>
<td>node1</td>
<td>vldb</td>
<td>154</td>
<td>154</td>
<td>14847</td>
<td>node0</td>
<td>secondary</td>
</tr>
<tr>
<td>node2</td>
<td>vldb</td>
<td>154</td>
<td>154</td>
<td>14847</td>
<td>node0</td>
<td>secondary</td>
</tr>
<tr>
<td>node3</td>
<td>vldb</td>
<td>154</td>
<td>154</td>
<td>14847</td>
<td>node0</td>
<td>secondary</td>
</tr>
</tbody>
</table>

4 entries were displayed.

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.

Example

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

<table>
<thead>
<tr>
<th>Time</th>
<th>Node</th>
<th>Severity</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/13/2013 14:03:51</td>
<td>node0</td>
<td>INFORMATIONAL</td>
<td>scsiblade.in.quorum: The scsi-blade ...</td>
</tr>
<tr>
<td>8/13/2013 14:03:51</td>
<td>node1</td>
<td>INFORMATIONAL</td>
<td>scsiblade.in.quorum: The scsi-blade ...</td>
</tr>
</tbody>
</table>

5. Return to the admin privilege level:

```
set -privilege admin
```

Related information

*Clustered Data ONTAP 8.3 System Administration Guide*

Verifying storage health

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

Steps

1. If you are preparing to upgrade, revert, or downgrade, verify disk status:

<table>
<thead>
<tr>
<th>To check for</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broken disks</td>
<td>a. Display any broken disks:</td>
</tr>
<tr>
<td></td>
<td>storage disk show -state broken</td>
</tr>
<tr>
<td>Disks undergoing maintenance or reconstruction</td>
<td>b. Remove or replace any broken disks.</td>
</tr>
<tr>
<td></td>
<td>a. Display any disks in maintenance, pending, or reconstructing states:</td>
</tr>
<tr>
<td></td>
<td>storage disk show -state maintenance</td>
</tr>
<tr>
<td></td>
<td>b. Wait for the maintenance or reconstruction operation to finish before proceeding.</td>
</tr>
</tbody>
</table>

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates:

```
storage aggregate show -state online
```
This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

Example

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

3. Verify that all volumes are online by displaying any volumes that are *not* online:

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

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

Example

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

Related information

*Clustered Data ONTAP 8.3 Logical Storage Management Guide*
*Clustered Data ONTAP 8.3 Physical Storage Management Guide*

Verifying that there is adequate free space in every volume containing LUNs

Before upgrading a cluster in a SAN environment, you must ensure that every volume containing LUNs has available at least 1 MB of free space. The space is needed to accommodate changes in the on-disk data structures used by the new version of Data ONTAP.

About this task

“LUNs” in this context refers to the LUNs that Data ONTAP serves to clients, not to the array LUNs used for storage on a storage array.

Steps

1. Determine which volumes contain LUNs:

```
lun show -fields volume
```

Example

```
cluster1::> lun show -fields volume
vserv path                                volume
--------- --------------------------------- ---------
vs1     /vol/vol1/lunA                  vol1
vs1     /vol/vol1/lunB                  vol1
vs1     /vol/vol1/lunC                  vol1
vs1     /vol/vol2/lunD                  vol2
vs1     /vol/vol2/lunE                  vol2
```

2. For each volume that contains a LUN, check the free space in the volume:

```
df -volume volume_name
```

Example

```
cluster1::> df -volume vol1
Filesystem           kbytes   used    avail capacity Mounted on Vserver
/vol/vol1/          498073600  6380492  388158972      22%  --- vs1
/vol/vol1/.snapshot  26214400   17364  26197036      0%  --- vs1
2 entries were displayed.
```

3. If the volume does not have at least 1 MB (1,024 KB) of free space, create free space in the full volume either by deleting unnecessary data or by growing the size of the volume.
Related information

Clustered Data ONTAP 8.3 Logical Storage Management Guide

Verifying networking and storage status for MetroCluster configurations

Before and after performing a minor upgrade or downgrade in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

About this task

If you are performing a major upgrade from Data ONTAP 8.2, you do not need to complete this procedure.

Steps

1. Verify the LIF status:

   ```
   network interface show
   ```

   In normal operation, LIFs for source SVMs must be up and located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs should be up, but they do not need to be located on their home nodes.

Example

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Is</th>
<th>Port</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1-a1_clus1</td>
<td>up/up</td>
<td></td>
<td>192.0.2.1/24</td>
<td>cluster1-01</td>
<td>e2a</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_clus2</td>
<td>up/up</td>
<td></td>
<td>192.0.2.2/24</td>
<td>cluster1-01</td>
<td>e2b</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_clus1</td>
<td>up/up</td>
<td></td>
<td>192.0.2.3/24</td>
<td>cluster1-02</td>
<td>e2a</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_clus2</td>
<td>up/up</td>
<td></td>
<td>192.0.2.4/24</td>
<td>cluster1-02</td>
<td>e2b</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_mgmt1</td>
<td>up/up</td>
<td></td>
<td>198.51.100.1/24</td>
<td>cluster1-01</td>
<td>e3a</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_inet4_intercluster1</td>
<td>up/up</td>
<td></td>
<td>198.51.100.2/24</td>
<td>cluster1-01</td>
<td>e3c</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_inet4_intercluster2</td>
<td>up/up</td>
<td></td>
<td>198.51.100.3/24</td>
<td>cluster1-01</td>
<td>e3c</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_mgmt1</td>
<td>up/up</td>
<td></td>
<td>198.51.100.4/24</td>
<td>cluster1-01</td>
<td>e0M</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_inet4_intercluster1</td>
<td>up/up</td>
<td></td>
<td>198.51.100.5/24</td>
<td>cluster1-02</td>
<td>e3c</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_inet4_intercluster2</td>
<td>up/up</td>
<td></td>
<td>198.51.100.6/24</td>
<td>cluster1-02</td>
<td>e3d</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_mgmt1</td>
<td>up/up</td>
<td></td>
<td>198.51.100.7/24</td>
<td>cluster1-02</td>
<td>e0M</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_data1</td>
<td>up/up</td>
<td></td>
<td>198.51.100.8/24</td>
<td>cluster1-01</td>
<td>e3a</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_data2</td>
<td>up/up</td>
<td></td>
<td>198.51.100.9/24</td>
<td>cluster1-01</td>
<td>e3d</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_data3</td>
<td>up/up</td>
<td></td>
<td>198.51.100.10/24</td>
<td>cluster1-01</td>
<td>e3c</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_data4</td>
<td>up/up</td>
<td></td>
<td>198.51.100.11/24</td>
<td>cluster1-01</td>
<td>e3a</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_data1</td>
<td>up/up</td>
<td></td>
<td>198.51.100.12/24</td>
<td>cluster1-01</td>
<td>e3d</td>
<td>true</td>
<td></td>
</tr>
</tbody>
</table>
2. Verify the state of the aggregates:

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

This command displays any aggregates that are not online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

**Example**

This example shows a cluster in normal operation:

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

**Example**

This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are offline:

```bash
cluster1::> storage aggregate show -state !online

<table>
<thead>
<tr>
<th>Aggregate</th>
<th>Size</th>
<th>Available</th>
<th>Used %</th>
<th>State</th>
<th>#Vols</th>
<th>Nodes</th>
<th>RAID Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggr0_b1</td>
<td>0B</td>
<td>0B</td>
<td>0%</td>
<td>offline</td>
<td>0</td>
<td>cluster2-01</td>
<td>raid_dp, mirror</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>degraded</td>
</tr>
<tr>
<td>aggr0_b2</td>
<td>0B</td>
<td>0B</td>
<td>0%</td>
<td>offline</td>
<td>0</td>
<td>cluster2-02</td>
<td>raid_dp, mirror</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>degraded</td>
</tr>
</tbody>
</table>
```

2 entries were displayed.

3. Verify the state of the volumes:

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

This command displays any volumes that are not online. In normal operation, all root and data volumes owned by the local cluster's SVMs must be online. However, if the MetroCluster configuration is in switchover, all volumes must be online.
Example

This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.

```bash
cluster1::> volume show -state !online
(volume show)
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- ----- 
vs2-mc    vol1         aggr1_b1     -          RW            -          -     -
vs2-mc    root_vs2     aggr0_b1     -          RW            -          -     -
vs2-mc    vol2         aggr1_b1     -          RW            -          -     -
vs2-mc    vol3         aggr1_b1     -          RW            -          -     -
vs2-mc    vol4         aggr1_b1     -          RW            -          -     -
5 entries were displayed.
```

Related concepts

*Upgrade requirements for MetroCluster configurations* on page 27

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:
   ```bash
   volume show -is-sis-volume true
   
   Example
   ``
   
   This example displays a deduplicated volume and the aggregate that contains it.

   ```bash
   cluster1::> volume show -is-sis-volume true
   (volume show)
   Vserver   Volume       Aggregate    State      Type       Size  Available Used%
   --------- ------------ ------------ ---------- ---- ---------- ---------- ----- 
   vs1       vol_2        aggr_2       online     RW         20GB    18.74GB    6%
   
   2 entries were displayed.
   ```

2. Determine the free space available on each volume that you identified:
   ```bash
   df -vserver Vserver_name -volume volume_name
   
   Example
   
   In this example, the capacity field displays the percentage of used space on the deduplicated volume identified earlier (vol_2):
   ```
   ```bash
   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.
   ```

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. If necessary, you can increase the sizes of any aggregates that exceed this capacity.

Clustered Data ONTAP 8.3 Physical Storage Management Guide

Example

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

| Cluster | df -A -aggregate aggr_2
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggr_2</td>
<td>kbytes</td>
</tr>
<tr>
<td>aggr_2</td>
<td>344220000</td>
</tr>
<tr>
<td>aggr_2/.snapshot</td>
<td>0</td>
</tr>
</tbody>
</table>

2 entries were displayed.

Verifying the LIF failover configuration

Before you perform an upgrade, you must verify that the failover policies and failover groups are configured correctly.

Steps

1. Display the failover policy for each data port:

   network interface show -role data -failover

   Example

   This example shows the default failover configuration for a two-node cluster with two data LIFs running Data ONTAP 8.2.x:

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Interface</th>
<th>Home Port</th>
<th>Failover Policy</th>
<th>Failover Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>lif0</td>
<td>node0:e0b</td>
<td>nextavail</td>
<td>system-defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Failover Targets: node0:e0b, node0:e0c, node0:e0d, node0:e0e, node0:e0f, node1:e0c, node1:e0d, node1:e0e, node1:e0f</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>lif1</td>
<td>node1:e0b</td>
<td>nextavail</td>
<td>system-defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Failover Targets: node1:e0b, node1:e0c, node1:e0d, node1:e0e, node1:e0f, node0:e0c, node0:e0d, node0:e0e, node0:e0f</td>
<td></td>
</tr>
</tbody>
</table>

The Failover Targets field shows a prioritized list of failover targets for each LIF. For example, if lif0 fails over from its home port (e0b on node0), it first attempts to fail over to port e0c on node0. If lif0 cannot fail over to e0c, it next attempts to fail over to port e0d on node0, and so on.

2. If you have LIFs on multiple IP subnets, verify that each LIF belongs to a failover group that contains ports on the same layer 2 broadcast domain.

   A user-defined failover group must be configured for each VLAN or broadcast domain, and each LIF must subscribe to the corresponding failover group.

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.

5. If you are preparing for a major upgrade, verify that the ports in each failover group have the same MTU value.

During the upgrade to the Data ONTAP 8.3 release family, Data ONTAP automatically creates broadcast domains based on your failover group configuration. This requires that the data ports in each failover group have the same MTU value as defined by RFC 1042, or the upgrade will fail.

**Note:** This requirement does not apply to the e0M port, which has a maximum MTU value of 1500. The upgrade will not fail if the e0M port has a different MTU value from the other ports in its failover group.

a. Determine the MTU value of each data and node management port in the cluster:

```bash
classport show
```

**Example**

In this example, the `e0a` and `e0b` ports have different MTU values:

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>Role</th>
<th>Link</th>
<th>MTU Admin/Oper</th>
<th>Duplex Admin/Oper</th>
<th>Speed (Mbps) Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>e0M</td>
<td>node-mgmt</td>
<td>up</td>
<td>1500</td>
<td>true/false</td>
<td>full/full</td>
</tr>
<tr>
<td></td>
<td>e0a</td>
<td>data</td>
<td>up</td>
<td>9000</td>
<td>true/false</td>
<td>full/full</td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>data</td>
<td>up</td>
<td>1500</td>
<td>true/false</td>
<td>full/full</td>
</tr>
<tr>
<td></td>
<td>e1a</td>
<td>cluster</td>
<td>up</td>
<td>9000</td>
<td>true/false</td>
<td>full/full</td>
</tr>
<tr>
<td></td>
<td>e1b</td>
<td>cluster</td>
<td>up</td>
<td>9000</td>
<td>true/false</td>
<td>full/full</td>
</tr>
</tbody>
</table>

b. If any of the ports have different MTU values, verify that each failover group contains ports with the same MTU value:

```bash
network interface failover-groups show
```

**Example**

In this example, the `clusterwide` failover group contains all data and node management ports. However, this configuration will cause the upgrade to fail, because the `e0a` and `e0b` ports have different MTU values.

<table>
<thead>
<tr>
<th>Failover Group</th>
<th>Node</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>clusterwide</td>
<td>node0</td>
<td>e0M</td>
</tr>
<tr>
<td></td>
<td>node0</td>
<td>e0a</td>
</tr>
<tr>
<td></td>
<td>node0</td>
<td>e0b</td>
</tr>
<tr>
<td></td>
<td>node1</td>
<td>e0M</td>
</tr>
<tr>
<td></td>
<td>node1</td>
<td>e0a</td>
</tr>
<tr>
<td></td>
<td>node1</td>
<td>e0b</td>
</tr>
</tbody>
</table>

b. If any failover groups contain data ports with multiple MTU values, do one of the following for each port:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove the port from its failover group and add it to a different failover group with the same MTU value.</td>
<td>a. Remove the port from its failover group:</td>
</tr>
<tr>
<td></td>
<td>network interface failover-groups delete -failover-group failover_group_name -node node_name -port port</td>
</tr>
<tr>
<td></td>
<td>b. Add the port to a new failover group, or an existing failover group that contains ports with the same MTU value:</td>
</tr>
<tr>
<td></td>
<td>network interface failover-groups create -failover-group failover_group_name -node node_name -port port</td>
</tr>
<tr>
<td>Update the port's MTU value to match the other ports in the failover group.</td>
<td>network port modify -node node_name -port port -mtu MTU_size</td>
</tr>
</tbody>
</table>

**Related information**

*IETF RFC 1042: A Standard for the Transmission of IP Datagrams over IEEE 802 Networks*

*Clustered Data ONTAP 8.3 Network Management Guide*

**Verifying the SAN configuration**

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

**Steps**

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

2. Verify that each host is connected to a LIF on each node.
   
   You should record the list of initiators for comparison after the upgrade.

   **For...** | **Enter...**
---|---
| iSCSI | iscsi initiator show -fields igroup,initiator-name,tpgroup |
| FC | fcp initiator show -fields igroup,wwpn,lif |

**Verifying the system time**

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

**Steps**

1. Verify that the cluster is associated with an NTP server:

   **If you are running...** | **Enter this command...**
---|---
| Data ONTAP 8.2.x | system services ntp server show |
| Data ONTAP 8.3.x | cluster time-service ntp server show |

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

Related information

*Clustered Data ONTAP 8.3 System Administration Guide*

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

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
```

**Preparing Data ONTAP features for the upgrade**

Some Data ONTAP features have configuration requirements that must be completed before the cluster can be upgraded.

**Removing oversized local UNIX user and group names**

Beginning with Data ONTAP 8.3, there is a limit of 64 characters for local UNIX user and group names. You can no longer create new user and group names with more than 64 characters, and you must remove existing user and group names with more than 64 characters before upgrading. Name mappings using oversized names will fail after upgrading.

**Steps**

1. Check the list of existing local UNIX users and groups for names that are longer than 64 characters:

   ```
   vserver services unix-user show
   vserver services unix-group show
   ```

2. Delete any users and groups with names longer than 64 characters:

   ```
   vserver services unix-user delete -vserver vserver_name -user user_name
   vserver services unix-group delete -vserver vserver_name -name group_name
   ```

3. Re-create any needed users or groups with names that are no longer than 64 characters:

   ```
   vserver services unix-user create -vserver vserver_name -user user_name
   -id user_ID -primary-gid primary_group_ID
   vserver services unix-group create -vserver vserver_name -name group_name -id group_ID
   ```

4. Verify that no oversized UNIX user and group names remain:

   ```
   vserver services unix-user show
   vserver services unix-group show
   ```

   After upgrading, if you receive an EMS message indicating that oversized names were detected, repeat these steps to identify, delete, and re-create any remaining oversized user and group names.

5. Modify any existing name mappings to use the new user and group names as needed.
Verifying that the netgroup file is present on all nodes

If you have loaded netgroups into Storage Virtual Machines (SVMs), before you upgrade or revert, you must verify that the netgroup file is present on each node. A missing netgroup file on a node can cause an upgrade or revert to fail.

About this task
For more information about netgroups and loading them from a URI, see the Clustered Data ONTAP File Access Management Guide for NFS.

Steps
1. Set the privilege level to advanced:
   ```bash
   set -privilege advanced
   ```
2. Display the netgroup status for each SVM:
   ```bash
   vserver services netgroup status
   ```
3. Return to the admin privilege level:
   ```bash
   set -privilege admin
   ```
4. Verify that for each SVM, each node shows the same netgroup file hash value.
   If this is the case, you can skip the next step and proceed with the upgrade or revert. Otherwise, proceed to the next step.
5. On any one node of the cluster, manually load the netgroup file to ensure that they are consistent across all nodes:
   ```bash
   vserver services netgroup load -vserver vserver_name -source uri
   ```
   This command downloads the netgroup file on all nodes. If a netgroup file already exists on a node, it is overwritten.

Converting the volume guarantee for volumes with a guarantee type of file

If your system includes volumes with a guarantee of file that contain space-reserved LUNs or files, and you need the reservations for those LUNs or files to be honored immediately after the upgrade is complete, you should change the space guarantee type of those volumes to volume before you upgrade.

About this task
This task is optional at this point in the upgrade process. You can choose to manually enable your disabled guarantees, if any, after the upgrade is complete. However, if you have critical workloads that use space-reserved LUNs or files in file-guaranteed volumes, you should complete this procedure before the upgrade.

The volume guarantee type of file is not supported for Data ONTAP 8.3 and later. Volumes with a volume guarantee of file are converted during the upgrade according to whether they contain any space-reserved LUNS or files:

- If the volume contains no space-reserved LUNs or files, its volume guarantee is converted to none
- If the volume contains space-reserved LUNs or files, its volume guarantee is converted to volume.
However, because there might not be enough free space available to honor the volume guarantee, the volume guarantee is initially disabled. You must enable it manually before the space-reserved LUN or file has the same space protections it had before the upgrade.

If any of the affected volumes contained free space or unreserved files before the upgrade, those volumes consume additional space from the aggregate when their guarantee is enabled.

Steps
1. Determine whether you have any volumes with a volume type of `file`
   
   ```
   volume show -space-guarantee file
   ```
   
   All volumes on your cluster with a volume type of `file` are displayed.

2. If any of the volumes displayed contain space-reserved LUNs or files, and you need those reservations to be honored immediately after the upgrade is complete, update their volume guarantee to `volume`:  
   
   ```
   volume modify -vserver vserver_name -volume volume_name -space-guarantee volume
   ```

3. If the `volume modify` command fails due to insufficient space, add storage to the aggregate or otherwise increase the free space available, and repeat the command.

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.

<table>
<thead>
<tr>
<th>Logical</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Is Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vserver</td>
<td>Interface</td>
<td>Admin/Oper</td>
<td>Network</td>
<td>Port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vs0</td>
<td>data001</td>
<td>up/up</td>
<td>192.0.2.120/24</td>
<td>node0</td>
</tr>
<tr>
<td></td>
<td>data002</td>
<td>up/up</td>
<td>192.0.2.121/24</td>
<td>node0</td>
</tr>
<tr>
<td></td>
<td>data003</td>
<td>up/up</td>
<td>192.0.2.122/24</td>
<td>node0</td>
</tr>
<tr>
<td></td>
<td>data004</td>
<td>up/up</td>
<td>192.0.2.123/24</td>
<td>node0</td>
</tr>
<tr>
<td></td>
<td>data005</td>
<td>up/up</td>
<td>192.0.2.124/24</td>
<td>node1</td>
</tr>
<tr>
<td></td>
<td>data006</td>
<td>up/up</td>
<td>192.0.2.125/24</td>
<td>node1</td>
</tr>
<tr>
<td></td>
<td>data007</td>
<td>up/up</td>
<td>192.0.2.126/24</td>
<td>node1</td>
</tr>
<tr>
<td></td>
<td>data008</td>
<td>up/up</td>
<td>192.0.2.127/24</td>
<td>node1</td>
</tr>
</tbody>
</table>

   8 entries were displayed.

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
Preparing SVM networking for a major upgrade

Before performing a major upgrade from Data ONTAP 8.2, you must configure a data LIF for each data SVM that can reach all external servers. You must also ensure that failover groups and routes are configured to enable these LIFs to reach all external servers throughout the upgrade.

Before you begin

• If the cluster has separate management and data networks, and if the external servers are only accessible from node management LIFs, then the cluster should be running Data ONTAP 8.2.2 GA or later.

Starting with Data ONTAP 8.2.2 GA, you can configure the data LIFs needed for external connectivity on node management ports.

Attention: If the cluster does not meet this requirement and you do not want to upgrade to Data ONTAP 8.2.2 GA, then you must have wired a data port on each of the first two nodes to a network that can reach the external servers.

• You must have a permanent IP address available for each SVM management LIF that you plan to create.

About this task

You must perform this procedure before installing the target Data ONTAP software images. The image installation does not succeed until all of the data LIFs needed for external server connectivity, failover groups, and routes are configured.

After a node is upgraded to Data ONTAP 8.3, SVMs can initiate connections only to the following external servers through their own LIFs:

• DNS, NIS, and LDAP servers

• Active Directory servers

• Kerberos servers

• Domain controllers

Example

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

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

1. Display the data SVMs in the cluster:

   `vserver show -type data -admin-state running`

   You must configure an existing data LIF or create an SVM management LIF for each SVM in the cluster.

   Example

   ```
   cluster1::> vserver show -type data -admin-state running
   Admin     Root                  Name    Name
   Vserver     Type    State     Volume     Aggregate  Service Mapping
   ----------- ------- --------- ---------- ---------- ------- -------
   vs0         data    running   vs0_root   aggr1      file,   file
   nis
   vs1         data    running   vs1_root   aggr3      file    file
   vs2         data    running   vs2_root   aggr2      ldap    file
   3 entries were displayed.
   ```

2. For each SVM, determine which external services the SVM is using.

   You should record the IP address of each external server that is configured for this SVM.

   To check for this external service... Enter this command...

<table>
<thead>
<tr>
<th>DNS</th>
<th>vserver services dns show -vserver Vserver_name -state enabled -fields name-servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIS</td>
<td>vserver services nis-domain show -vserver Vserver_name -active true -fields servers</td>
</tr>
</tbody>
</table>

   **LDAP**

   a. Find the list of client configurations:

   ```
   vserver services ldap show -vserver Vserver_name -client-enabled true -fields client-config
   ```

   b. Display the servers in each client configuration:

   ```
   vserver services ldap client show -vserver Vserver_name -client-config client_config_name -client-enabled true -fields servers
   ```

   **LDAP (preferred servers)**

   a. Find the list of client configurations:

   ```
   vserver services ldap show -vserver Vserver_name -client-enabled true -fields client-config
   ```

   b. Display the servers in each client configuration:

   ```
   vserver services ldap client show -vserver Vserver_name -client-config client_config_name -client-enabled true -fields preferred-ad-servers
   ```

   **Kerberos**

   `vserver services kerberos-realm show`
To check for this external service...

<table>
<thead>
<tr>
<th>Service</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td><code>vserver services kerberos-realm show -fields adserver-ip</code></td>
</tr>
<tr>
<td>Admin server</td>
<td><code>vserver services nfs kerberos-realm show -fields adminserver-ip</code></td>
</tr>
<tr>
<td>Password server</td>
<td><code>vserver services nfs kerberos-realm show -fields passwordserver-ip</code></td>
</tr>
<tr>
<td>Domain controller (preferred)</td>
<td><code>vserver cifs domain preferred-dc show -vserver Vserver_name -fields preferred-dc</code></td>
</tr>
<tr>
<td>Domain controller (discovered)</td>
<td><code>vserver cifs domain discovered-servers show -vserver Vserver_name -fields address</code></td>
</tr>
<tr>
<td>iSNS</td>
<td><code>vserver iscsi isns show -vserver Vserver_name</code></td>
</tr>
<tr>
<td>Policy server (primary)</td>
<td><code>vserver fpolicy policy external-engine show -vserver Vserver_name -fields primary-servers</code></td>
</tr>
<tr>
<td>Policy server (secondary)</td>
<td><code>vserver fpolicy policy external-engine show -vserver Vserver_name -fields secondary-servers</code></td>
</tr>
</tbody>
</table>

3. Display the existing data LIFs for each SVM:

`network interface show -role data`

**Example**

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

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Is Name</th>
<th>Port</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>datalif1</td>
<td>up/up</td>
<td>192.0.2.100/24</td>
<td>node0</td>
<td>e0a</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td></td>
<td>datalif2</td>
<td>up/up</td>
<td>192.0.2.101/24</td>
<td>node1</td>
<td>e0b</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>datalif3</td>
<td>up/up</td>
<td>192.0.2.140/24</td>
<td>node0</td>
<td>e0a</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td></td>
<td>datalif4</td>
<td>up/up</td>
<td>192.0.2.146/24</td>
<td>node1</td>
<td>e0b</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>vs2</td>
<td>datalif5</td>
<td>up/up</td>
<td>192.0.2.142/24</td>
<td>node0</td>
<td>e0a</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td></td>
<td>datalif6</td>
<td>up/up</td>
<td>192.0.2.155/24</td>
<td>node1</td>
<td>e0b</td>
<td>true</td>
<td></td>
</tr>
</tbody>
</table>

6 entries were displayed.
```

4. For each SVM, determine which data LIF or LIFs to use for external server connectivity.

If the SVM cannot reach all of its configured external servers from a single LIF, you must configure multiple data LIFs for external server connectivity. For example, if the external servers are on multiple, disconnected networks, you should configure a separate LIF to reach the servers on each disconnected network.

**If...**

| The SVM has a data LIF with a network path to each of its configured external servers |
|-----------------------------------|-----------------------------------|
| Then...                           | Record the data LIF. You can modify this LIF for external server connectivity. |
If... Then...

None of the data LIFs have a network path to the external servers

Choose an IP address for a new SVM management LIF. The IP address must be on a subnet that enables the LIF to reach each of the external servers.

If the external servers use both IPv4 and IPv6 addresses, you must choose both an IPv4 address and an IPv6 address.

5. Determine which node you plan to upgrade first.

All of the SVM data LIFs that you configure for external connectivity must be hosted on the first node that you upgrade. When you install the Data ONTAP 8.3 image on this node, the image installation does not succeed unless Data ONTAP can verify that these LIFs are located on the node.

6. Configure a failover group for the data LIFs.

You must configure a failover group to ensure that the data LIFs are located on the correct ports during the upgrade. When you configure the data LIFs for external connectivity, you assign them to this failover group.

a. Determine whether an appropriate failover group exists for the data LIFs needed for external connectivity:

   `network interface failover-groups show`

   The LIFs must belong to a failover group that includes ports on the first node to be upgraded and its HA partner. If the data ports are on different VLANs or broadcast domains, a separate failover group should exist for each VLAN or broadcast domain.

   **Example**

   In this example, the LIFs can use the `clusterwide` failover group, because it contains ports only on the first HA pair:

   ```
   cluster1::> network interface failover-groups show
   Failover Group               Node    Port
   -------------------     ----------
   clusterwide
      node0       e0a
      node0       e0b
      node1       e0a
      node1       e0b
   4 entries were displayed
   ```

b. If no appropriate failover groups exist, use the `network interface failover-groups create` command to create a new failover group.

   The failover group should include the data ports on the first node to be upgraded and its HA partner. If the data ports are on different VLANs or broadcast domains, you should create a separate failover group for each VLAN or broadcast domain.

   **Example**

   In this example, a new failover group is created with all of the data ports on the first node and its HA partner:

   ```
   cluster1::> network interface failover-groups create -failover-group lif_sufficiency -node node0 -port e0a
   cluster1::> network interface failover-groups create -failover-group lif_sufficiency -node node0 -port e0b
   cluster1::> network interface failover-groups create -failover-group lif_sufficiency -node node1 -port e0a
   ```
7. For each SVM, configure a data LIF for external server connectivity.

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an existing data LIF for external server connectivity</td>
<td>Modify the data LIF:</td>
</tr>
<tr>
<td></td>
<td>network interface modify -vserver Vserver_name -lif LIF_name -home-node first_node_to_upgrade -home-port port -auto-revert true -failover-group failover_group_name -failover-policy nextavail</td>
</tr>
<tr>
<td></td>
<td>This command modifies the LIF to be located on the first node to be upgraded, to automatically revert to the home node as soon as it boots Data ONTAP 8.3, and to use the failover group that you previously configured.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create a new SVM management LIF</th>
<th>Create a new LIF:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>network interface create -vserver Vserver_name -lif LIF_name -data-protocol none -role data -home-node first_node_to_upgrade -home-port port -address IP_address -netmask netmask_address -status-admin up -auto-revert true -failover-group failover_group_name -failover-policy nextavail</td>
</tr>
<tr>
<td></td>
<td>This command creates an SVM management LIF on the first node to be upgraded. The LIF is set to automatically revert so that it immediately reverts to the home node as soon as the node boots Data ONTAP 8.3, and a failover group is assigned so that the LIF fails over only to a port on the first HA pair.</td>
</tr>
<tr>
<td></td>
<td>If the external servers use IPv4 addresses, you must create the LIF with an IPv4 address. If they use IPv6 addresses, you must create the LIF with an IPv6 address. If they use both IPv4 and IPv6 addresses, you must create two LIFs for the SVM: one with an IPv4 address, and another with an IPv6 address.</td>
</tr>
</tbody>
</table>

8. For each data LIF that you configured, verify that the LIF has a default route to the subnet on which the external servers reside:

a. Find the routing group that the data LIF is associated with:

   network interface show -vserver Vserver_name -lif data_LIF_name -fields routing-group

   **Example**

   ```
   cluster1::> network interface show -vserver vs0 -lif datalif1 -fields routing-group
   vserver lif routing-group
   --------- --------- --------------
   vs0      datalif1  d203.0.113.1/24
   ```
b. Display the routes in the routing group:

```
network routing-group route show -vserver Vserver_name -routing-group routing-group_name
```

**Example**

```
cluster1::> network routing-group route show -vserver vs0 -routing-group d203.0.113.1/24
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Group</th>
<th>Destination</th>
<th>Gateway</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>d203.0.113.1/24</td>
<td>0.0.0.0/0</td>
<td>198.51.100.5</td>
<td>20</td>
</tr>
</tbody>
</table>

C. If the external servers reside on a different subnet from the data LIF that you configured, and a default route does not exist, create a new route to the subnet's gateway:

```
network routing-groups route create -vserver Vserver_name -routing-group routing-group_name -destination 0.0.0.0/0 -gateway gateway_address
```

**Example**

```
cluster1::> network routing-groups route create -vserver vs0 -routing-group d203.0.113.1/24 -destination 0.0.0.0/0 -gateway 198.51.100.5
```

**Related concepts**

*SVM networking considerations for major upgrades* on page 23

**Related tasks**

*Installing Data ONTAP software images for a major upgrade* on page 56

Before performing a major upgrade to Data ONTAP 8.3, you must install the software image on the first node to verify that each SVM will be able to reach its external servers during the upgrade. After the image installation succeeds, you install the software image on the remaining nodes.

**Removing FlexCache volumes**

Before upgrading to Data ONTAP 8.3, you must identify and remove any FlexCache volumes.

**About this task**

FlexCache volumes are not supported in Data ONTAP 8.3. If you upgrade to Data ONTAP 8.3 with any FlexCache volumes, they are taken offline automatically.

**Steps**

1. Identify any FlexCache volumes:

```
volume flexcache show
```

**Example**

```
cluster1::> volume flexcache show

-------------------------Cache-------------- Conn.-----Origin-----------
Vserver Volume Aggregate Size  State  Available Status Volume Aggregate State
------- ------ --------- ----- ------ --------- ------ --------- ----- 
vs1    dst_cache_01
       node01_aggr

                                20MB online  19.91MB    ok dst  node02_aggr
```
2. Delete each FlexCache volume:

```
volume flexcache delete -vserver vserver_name -origin-volume volume_name
```

**Example**

```
cluster1::> volume flexcache delete -vserver vs1 -origin-volume dst
Successfully deleted cache volume "dst_cache_01".
Successfully deleted cache volume "dst_cache_02".
The origin volume "dst" is no longer cached in the cluster.
```

**Identifying active CIFS sessions that should be terminated**

Before performing a nondisruptive upgrade or downgrade, 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 or Microsoft SQL Server clients using the SMB 3.0 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: CIFSLAB\user1
UNIX User: nobody
Open Shares: 1
Open Files: 2
Open Other: 0
Connected Time: 8m 39s
Idle Time: 7m 45s
Protocol Version: SMB2_1
Continuously Available: No
1 entry was displayed.
```

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
```

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Mode</th>
<th>Volume</th>
<th>Share</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Regular</td>
<td>rw</td>
<td>vol10</td>
<td>homedirshare</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Regular</td>
<td>rw</td>
<td>vol10</td>
<td>homedirshare</td>
<td>No</td>
</tr>
</tbody>
</table>

Path: \TestDocument.docx
Path: \file1.txt
2 entries were displayed.

Related concepts

Considerations for session-oriented protocols on page 171

Preparing all load-sharing mirrors for a major upgrade

Before performing a major upgrade from Data ONTAP 8.2, you should move all of the load-sharing mirror source volumes to an aggregate on the node that you will upgrade last. This ensures that load-sharing mirror destination volumes are the same or later versions of Data ONTAP.

Steps

1. Record the locations of all load-sharing mirror source volumes.
   Knowing where the load-sharing mirror source volumes came from will help facilitate returning them to their original locations after the major upgrade.

2. Determine the node and aggregate to which you will move the load-sharing mirror source volumes.

3. Move the load-sharing mirror source volumes to the node and aggregate by using the `volume move start` command.

Preparing SnapMirror relationships for a nondisruptive upgrade or downgrade

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

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

This example quiesces transfers involving the destination volume `vol1` from SVM `vs0.example.com`:

```
cluster1::> snapmirror quiesce -destination-path vs0.example.com:vol1
```
3. Verify that all SnapMirror relationships are quiesced:

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

This command displays any SnapMirror relationships that are not quiesced.

**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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait for the transfers to complete before performing the Data ONTAP upgrade.</td>
<td>Once each transfer completes, the relationship changes to Quiesced status.</td>
</tr>
<tr>
<td>Stop the transfers by entering the following command:</td>
<td>This command stops the SnapMirror transfer and restores the destination volume to the last Snapshot copy that was successfully transferred. The relationship is set to Quiesced status.</td>
</tr>
</tbody>
</table>

```
snapmirror abort -destination-path destination -h
```

**Note:** You must use the -foreground true parameter if you are aborting load-sharing mirror transfers.

**Related concepts**

*Upgrade requirements for SnapMirror* on page 25

**Related information**

*Clustered Data ONTAP 8.3 Data Protection Guide*

**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.

**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, 831_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

NetApp Downloads: Software

Installing Data ONTAP software images for a major upgrade

Before performing a major upgrade to Data ONTAP 8.3, you must install the software image on the first node to verify that each SVM will be able to reach its external servers during the upgrade. After the image installation succeeds, you install the software image on the remaining nodes.

Before you begin

- You must have prepared the SVM networking for a major upgrade by creating the necessary SVM management LIFs, failover groups, and routes.
- If a firewall is configured between the cluster and the external servers:
  - The firewall must accept ICMP packets from the data LIFs that you configured for external server connectivity. When you install the Data ONTAP 8.3 image on the first node, Data ONTAP attempts to ping each external server using ICMP packets to verify the networking configuration. If the firewall filters out the ICMP packets, the image installation will fail. To resolve this issue, you can open the firewall to accept ICMP packets for the IP addresses of the data LIFs that you configured for external server connectivity. You can close the firewall after the upgrade is complete.
  - The firewall must allow all data LIFs to reach external servers using their TCP/UDP service ports.
- You must have obtained the Data ONTAP software images.

About this task

You do not need to perform this procedure if you are using the automated method to perform a minor NDU or downgrade. In these cases, the cluster image update command automatically distributes and installs the target Data ONTAP image on each node in the cluster during the upgrade or downgrade.

When you install the software image on the first node, Data ONTAP checks your networking configuration to ensure that it satisfies the following conditions:

- Each SVM will be able to reach its external servers after the upgrade is complete.
- The first node to be upgraded hosts sufficient LIFs to enable each SVM to reach its external servers through the node.
- The second node to be upgraded (the first node's high-availability partner) is capable of hosting sufficient LIFs if the first node unexpectedly goes out of service during the upgrade.

This check is only performed when you install the software image on the first node. After the image installation succeeds on the first node and the SVM networking configuration is verified, the check is not run when you install the software image on the remaining nodes.

Steps

1. Install the software image on the first node to be upgraded:

   `system node image update -node node_name -package location -replace-package true`
You must install the software image on the same node on which you created the SVM management LIFs. This command downloads the software image and checks the networking configuration. If the networking configuration is validated, then the image is installed on the node. Otherwise, the command fails and provides a list of preconditions that you must address.

**Note:** The `system node image update` command might time out before the networking configuration has been validated. If the command output indicates that time expired, you should make the required networking configuration changes and then reenter the command to complete the remaining networking validation checks.

**Example**

In this example, the image installation fails because the first node does not host sufficient LIFs to ensure connectivity throughout the upgrade:

```bash
cluster1::> system node image update -node node0 -package http://www.example.com/downloads/x86-64/830_image.tgz -replace-package true

Software update started on node node0. Updating image2 with package http://www.example.com/downloads/x86-64/830_image.tgz.
Download package. This may take up to 10 minutes.
99% downloaded
100% downloaded
Download complete.
Listing package contents.
Decompressing package contents.
Invoking script (validation phase).
INSTALL running in check-only mode: the image will be validated only
Mode of operation is UPDATE
Current image is image1
Alternate image is image2
Package MD5 checksums pass
Versions are compatible
Available space on boot device is 1563 MB
Required space on boot device is 475 MB
Kernel binary matches install machine type
Checking ALL Vservers for sufficiency LIFs.
Running in upgrade mode.
Running in report mode.
Checking Vserver(s) (vs0 vs1) for sufficiency LIFs.
After upgrade, Server DNS Server 198.51.100.1 WILL BE UNREACHABLE from Vserver vs1.

******************************************************************************
* *** FAILURES FOUND. ***
* You must correct these failures to avoid service disruptions.
* One way to avoid failures in most environments is to create a
  * Vserver management LIF, one for each Vserver, that has connectivity to all
    * external servers (infrastructure servers such as DNS/NIS/LDAP).
  * Add a route for this LIF, if necessary, to provide connectivity to servers.
  * This LIF's home-node should be the first node that will upgrade to 8.3.0.
  * The LIF should have a failover group that includes ONLY the home node
    * and its HA partner. It should have auto-revert enabled.
      *(Failover-group, failover-policy, and auto-revert may be set to other
        * values as desired AFTER the cluster upgrade is complete.)*
    * Command to add LIFs:
      * network interface create -vserver <Vserver_name> -lif <lif_name>
        * -role data -data-protocol none
        * -netmask-length <bits> -auto-revert true
    * Command to add routes:
      * network routing-groups route create -vserver <Vserver_name>
    * Commands to manage failover groups:
      * network interface failover-groups
      * network interface modify -vserver <Vserver_name> -lif <lif_name>
        * -failover-group <group_name>
        * Command to modify a LIF's failover policy:
          * network interface modify -vserver <Vserver_name> -lif <lif_name>
            * -failover-policy <policy>
        * Commands to modify a LIF's home node:
          * network interface modify -vserver <Vserver_name> -lif <lif_name>
            * -home-node <node_name> -home-port <port_name>
      * Command to modify a LIF's auto-revert settings:
        * network interface modify -vserver <Vserver_name> -lif <lif_name> -auto-revert true
      * Other corrective actions may include:
        * Remove any decommissioned external servers from the Vserver configuration.
        * Commands to show/modify/delete server configurations
```

Upgrading Data ONTAP clusters | 57
2. Make any required networking configuration changes, and then repeat Step 1.

3. Verify that the software image is downloaded and installed on the first node:

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

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

   **Example**

   In this example, the software image has been downloaded and installed successfully on the first node:

   ```
   cluster1:~> system node image show-update-progress -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 node0.
   1 entry was acted on.
   ```

4. Install the software image on the remaining nodes:

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

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

5. 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 two-node cluster in which the software image has been downloaded and installed successfully on both nodes.
Related concepts

*SVM networking considerations for major upgrades* on page 23

Related tasks

*Preparing SVM networking for a major upgrade* on page 47

Disabling the 32-bit capability

Before you can upgrade your cluster to Data ONTAP 8.3, you must remove all 32-bit data and disable the 32-bit capability. You must complete this task even if you have never created 32-bit aggregates on your cluster.

**Before you begin**

- You must have expanded all 32-bit aggregates on the cluster to the 64-bit format.
- All aggregates on the cluster must be online.

**About this task**

32-bit data can exist on your cluster even if you have expanded all of your aggregates to the 64-bit format.

Disabling the 32-bit capability (the last step of this task) should be done *only* when you are ready to install the new image and upgrade to the new version of Data ONTAP.

**Steps**

1. Enter the advanced privilege mode:
   
   set -privilege advanced

2. Check whether the 32-bit capability can be disabled:

   `storage aggregate 64bit-upgrade 32bit-disable -check`

   If the command output indicates that your cluster does not contain any 32-bit data, you can skip to step 4. Otherwise, proceed to the next step.

3. Take the appropriate action or actions depending on the output of the previous command:

   **If the command output indicated that you have...**

   **Then...**

   - Offline aggregates or volumes
     
     Bring them online and repeat the previous step.

     You can use the `-force` parameter to disable the 32-bit capability with offline volumes or aggregate, but you might not be able to bring them online again after you upgrade.
If the command output indicated that you have...
Then...

| 32-bit data in one or more aggregates | Find and remove the 32-bit data and repeat the previous step. |

4. Disable the 32-bit capability:

```bash
storage aggregate 64bit-upgrade 32bit-disable
```

The command output should indicate that your cluster does not contain any 32-bit data. If it does not, you must repeat this task.

5. Return to the administrative privilege level:

```bash
set -privilege admin
```

### Expanding an aggregate to the 64-bit format

If your system contains 32-bit aggregates, you must expand them to the 64-bit format before upgrading to Data ONTAP 8.3 or later versions, because those versions of Data ONTAP do not support the 32-bit format. This procedure is not supported for Data ONTAP 8.3 or later versions.

**Before you begin**

- If the aggregate contains destination volumes for a SnapMirror relationship with a 32-bit source volume, the aggregate containing the source volume must be expanded before expanding the aggregate containing the destination volume.
- All FlexCache volumes contained by the aggregate to be expanded must be destroyed before you initiate the expansion. FlexCache volumes are not supported for Data ONTAP 8.3 and later.

**About this task**

For volumes in a SnapMirror relationship, the destination volume inherits the format of the source volume while the mirror is intact. If the aggregate you are expanding contains a destination volume whose source is a 32-bit volume and you break the mirror before expanding the aggregate, the destination volume is expanded to the 64-bit format. However, if you reestablish the mirror and the source volume is still 32-bit, the destination volume returns to the 32-bit format. For this reason, you must expand the aggregate containing the source volume before reestablishing the SnapMirror relationship if you want to expand all 32-bit volumes in the aggregate to the 64-bit format.

**Steps**

1. Enter advanced privilege mode:

   ```bash
   set -privilege advanced
   ```

2. Initiate the expansion:

   ```bash
   storage aggregate 64bit-upgrade start -aggregate aggr_name
   ```

3. Take the appropriate action:

<table>
<thead>
<tr>
<th>If the command...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiates successfully</td>
<td>Proceed to the next step.</td>
</tr>
<tr>
<td>Indicates that one or more volumes could not be expanded because they did not have enough space</td>
<td>Retry the command, adding the <code>grow-all</code> option.</td>
</tr>
</tbody>
</table>
4. Display the status of the expansion:

```
storage aggregate 64bit-upgrade status -aggregate aggr_name
```

The current status of the expansion is displayed. When the message indicates that there is no upgrade in progress, the expansion is complete.

5. Optional: Confirm that all volumes in the aggregate are 64-bit format:

```
volume show -aggregate aggr_name -fields block-type
```

6. Return to administrative privilege mode:

```
set -privilege admin
```

**Result**

The aggregate is expanded to the 64-bit format. Even if all volumes are expanded, however, some 32-bit data can remain in the Snapshot copies. The presence of 32-bit data in the source volumes or in the Snapshot copies prevents an upgrade or transition to Data ONTAP 8.3 or later.

**Finding and removing 32-bit data from source volumes and Snapshot copies**

Even if you have expanded all of your aggregates to the 64-bit format, some 32-bit or mixed-format FlexVol volumes or Snapshot copies can remain. These volumes and Snapshot copies must be removed before your data can be accessed by a cluster running Data ONTAP 8.3 or later.

**Before you begin**

- You must have expanded all 32-bit aggregates on the cluster to the 64-bit format.

**About this task**

You must repeat the steps in this task for each aggregate that contains 32-bit data.

**Steps**

1. Enter advanced mode:

```
set -privilege advanced
```

2. Display the format of all volumes in the aggregate:

```
storage aggregate 64bit-upgrade status -include-all-volumes -aggregate aggr_name
```

Each volume in the aggregate is displayed with its format.

3. For each 32-bit or mixed-format volume, determine the reason that the volume has not been expanded to the 64-bit format, and then take the appropriate action.

If you cannot determine the reason that the volume was not expanded, retry the aggregate expansion.

<table>
<thead>
<tr>
<th>If the volume...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the destination of a SnapMirror relationship</td>
<td>Expand the aggregate containing the source volume to the 64-bit format.</td>
</tr>
</tbody>
</table>
If the volume… | Then…
---|---
Is a read-only volume (but not a SnapMirror destination) | Make the volume writable and retry the expansion, or destroy the volume.
Did not expand because of insufficient free space in the volume or aggregate | Increase the free space in the volume or aggregate and retry the expansion.

All 32-bit and mixed-format volumes in the aggregate are now 64-bit. You can confirm this by repeating the previous step.

4. Display all 32-bit Snapshot copies on the cluster:

```
volume snapshot show -fs-block-format !64-bit -fields fs-block-format
```

5. Remove the 32-bit Snapshot copies by using the `volume snapshot delete` command.

**Attention:** This action deletes the data in the Snapshot copies. You must be certain that you do not need to retain the Snapshot copies before you delete them. Alternatively, you can wait for the 32-bit Snapshot copies to be aged out. The amount of time this takes depends on your Snapshot copy schedule.

If a Snapshot copy is the base Snapshot copy for a FlexClone volume, you must split the FlexClone volume from its parent before you can remove the Snapshot copy.

All 32-bit Snapshot copies are removed. You can confirm this by repeating the previous step.

6. Return to the administrative privilege level:

```
set -privilege admin
```

**Performing the software upgrade**

To upgrade a cluster to a new Data ONTAP release, you must change the default boot image, choose an upgrade method, and then perform the steps for the upgrade method.

**Related concepts**

*Types of cluster upgrades* on page 17

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

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

**Before you begin**

You must have satisfied upgrade preparation requirements.

**About this task**

**Attention:** If you are performing a major upgrade, the first node to be upgraded must be the node on which you configured the data LIFs for external server connectivity and installed the first Data ONTAP image. If you upgrade a different node first, the SVMs might not be able to reach their external servers during the upgrade process.
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 be upgraded last. If the node that currently holds epsilon is not the node that you plan to upgrade last, you can use the `cluster modify` command to transfer epsilon to a different node.

2. **Upgrading the first node in an HA pair** on page 63

   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 68

   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. Repeat Steps 2 and 3 for each additional HA pair.

After you finish

You should complete post-upgrade tasks.

Related concepts

- *How epsilon affects the upgrade sequence for four-node clusters* on page 22

### 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.

About this task

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

Steps

1. If this is the first node in the cluster to be upgraded, trigger an AutoSupport notification:
   
   ```
   autosupport invoke -node * -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.

2. Set the Data ONTAP 8.3 software image to be the default image:
   
   ```
   system image modify {-node nodenameA -iscurrent false} -isdefault true
   ```

   This command uses an extended query to change the Data ONTAP 8.3 software image (which is installed as the alternate image) to be the default image for the node.

3. Verify that the Data ONTAP 8.3 software image is set as the default image:
   
   ```
   system image show
   ```

   **Example**

   This example shows that version 8.3.1 is set as the default image on the node node0:
4. Disable automatic giveback on the partner node if it is enabled:

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

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

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

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

   **Example**

   ```
   cluster1::> storage failover show -node nodenameB -fields auto-giveback
   node    auto-giveback
   --------- ------------
   node1    false
   1 entry was displayed.
   ```

6. 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 that the node has performed for NFS, CIFS, FC, and iSCSI clients since the node was last booted. For each protocol, you need to run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

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

   **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
   ```

7. Migrate the data LIFs in one of the following ways:
If this node... | Description
---|---
Hosts the data LIFs that you configured for external server connectivity during the upgrade preparation | Do not migrate the data LIFs required for external server connectivity, but migrate any other data LIFs to the appropriate destination node:

```
network interface migrate -vserver Vserver_name -lif LIF_name -source-node nodenameA -destination_node node
```

**Attention:** The data LIFs required for external server connectivity will be migrated automatically when you initiate the takeover. Manually migrating these LIFs away from the first node can prevent them from automatically reverting to the node when it reboots, which can cause a temporary service disruption.

Does not host data LIFs configured for external server connectivity | Migrate all of the data LIFs away from the node:

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

8. Use the `network interface show` command to verify any LIFs that you migrated.

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

**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   | e0a       | node1     | e0a       | up          | up          
vs0         | data002   | e0b       | node1     | e0b       | up          | up          
vs0         | data003   | e0b       | node1     | e0b       | up          | up          
vs0         | data004   | e0a       | node1     | e0a       | up          | up          
```

4 entries were displayed.

9. Initiate a takeover:

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

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

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

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

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 the **In takeover** state.

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

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

2 entries were displayed.
11. Wait at least 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 might take longer than 8 minutes, depending on the characteristics of the client applications.

12. Return the aggregates to the first node:

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

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

13. Verify that all aggregates have been returned:

   ```
   storage failover show-giveback
   ```

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

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

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

      *Clustered Data ONTAP 8.3 High-Availability Configuration Guide*

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

   c. Reenter the `storage failover giveback` command.

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

15. Wait at least 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 might take longer than 8 minutes, depending on the characteristics of the client applications.

16. Verify that the upgrade was 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 complete, from the node, run the `system node upgrade-revert` 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
      ```
17. 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.
```

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

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

```
network port show -node nodenameA
```

If you are upgrading from the Data ONTAP 8.2 release family, you must enter this command on a node that has been upgraded to Data ONTAP 8.3.

**Example**

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

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

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>e0M</td>
<td>Default</td>
<td>-</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0a</td>
<td>Default</td>
<td>-</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Default</td>
<td>-</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e1a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/10000</td>
</tr>
<tr>
<td></td>
<td>e1b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/10000</td>
</tr>
</tbody>
</table>

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 their operational status is up:

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

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Status</th>
<th>Interface</th>
<th>Admin/Oper</th>
<th>Network</th>
<th>Current Node</th>
<th>Current Is</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>up/up</td>
<td>data001</td>
<td>up/up</td>
<td>192.0.2.120/24</td>
<td>node0</td>
<td>e0a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data002</td>
<td>up/up</td>
<td>192.0.2.121/24</td>
<td>node0</td>
<td>e0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data003</td>
<td>up/up</td>
<td>192.0.2.122/24</td>
<td>node0</td>
<td>e0b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data004</td>
<td>up/up</td>
<td>192.0.2.123/24</td>
<td>node0</td>
<td>e0a</td>
</tr>
</tbody>
</table>

4 entries were displayed.

19. 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
```
20. Reenable automatic giveback on the partner node if it was previously disabled:

    storage failover modify -node nodenameB -auto-giveback true

After you finish

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

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. Set the Data ONTAP 8.3 software image to be the default image:

    system image modify (-node nodenameB -iscurrent false) -isdefault true

   This command uses an extended query to change the Data ONTAP 8.3 software image (which is installed as the alternate image) to be the default image for the node.

2. Verify that the Data ONTAP 8.3 software image is set as the default image:

    system image show

   Example

   This example shows that version 8.3.1 is set as the default image on the node:

<table>
<thead>
<tr>
<th>Node</th>
<th>Image</th>
<th>Is</th>
<th>Is</th>
<th>Install</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>image1</td>
<td>false</td>
<td>false</td>
<td>8.2.1</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>true</td>
<td>8.3.1</td>
</tr>
<tr>
<td>node1</td>
<td>image1</td>
<td>false</td>
<td>true</td>
<td>8.2.1</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>8.3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4 entries were displayed.</td>
</tr>
</tbody>
</table>

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

    storage failover modify -node nodenameA -auto-giveback false

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

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

    storage failover show -node nodenameA -fields auto-giveback

   Example

<table>
<thead>
<tr>
<th>node</th>
<th>auto-giveback</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>1 entry was displayed.</td>
</tr>
</tbody>
</table>

5. 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:
   \texttt{set \ -privilege \ advanced}

b. Mark epsilon false on the node:
   \texttt{cluster \ modify \ -node \ nodename \ -epsilon \ false}

c. Mark epsilon true on the first node that was upgraded:
   \texttt{cluster \ modify \ -node \ nodename \ -epsilon \ true}

d. Return to the admin privilege level:
   \texttt{set \ -privilege \ admin}

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

   \texttt{system \ node \ run \ -node \ nodenameB \ -command \ uptime}

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

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

7. Migrate the data LIFs in one of the following ways:

<table>
<thead>
<tr>
<th>If this node...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts the data LIFs that you configured for external server connectivity during the upgrade preparation</td>
<td>Do \textit{not} migrate the LIFs required for external server connectivity, but migrate any other data LIFs to the appropriate destination node: \texttt{network \ interface \ migrate \ -vserver \ Vserver_name \ -lif \ LIF_name \ -source-node \ nodenameB \ -destination-node \ node}</td>
</tr>
<tr>
<td>Does not host data LIFs configured for external server connectivity</td>
<td>Migrate all of the data LIFs away from the node: \texttt{network \ interface \ migrate-all \ -node \ nodenameB}</td>
</tr>
</tbody>
</table>

8. Use the \texttt{network \ interface \ show} command to verify the status of any LIFs that you migrated.

   For more information about parameters you can use to verify LIF status, see the \texttt{network \ interface \ show} man page.
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-oper
```

<table>
<thead>
<tr>
<th>vserver lif</th>
<th>home-node</th>
<th>home-port</th>
<th>curr-node</th>
<th>curr-port</th>
<th>status-oper</th>
<th>status-admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>data001</td>
<td>e0a</td>
<td>node1</td>
<td>e0a</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>vs0</td>
<td>data002</td>
<td>e0b</td>
<td>node0</td>
<td>e0b</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>vs0</td>
<td>data003</td>
<td>e0b</td>
<td>node0</td>
<td>e0b</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>vs0</td>
<td>data004</td>
<td>e0a</td>
<td>node0</td>
<td>e0a</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>

4 entries were displayed.

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

<table>
<thead>
<tr>
<th>If you are upgrading from a...</th>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data ONTAP 8.3.x release</td>
<td><code>storage failover takeover -ofnode nodenameB</code></td>
</tr>
<tr>
<td>Data ONTAP 8.2.x release</td>
<td><code>storage failover takeover -ofnode nodenameB - option allow-version-mismatch</code></td>
</tr>
</tbody>
</table>

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

The 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.

10. Verify that the takeover was successful:

    `storage failover show`

    If you are performing a major upgrade, with the first node running the newer version of Data ONTAP and the partner running an earlier Data ONTAP release family, the nodes are in a state of version mismatch. This means that normal high-availability functions such as NVRAM mirroring and automatic takeover are not in effect. You might see error messages indicating version mismatch and mailbox format problems. This is expected behavior; it represents a temporary state in a major nondisruptive upgrade and is not harmful. You should complete the upgrade procedure as quickly as possible; do not allow the two nodes to remain in a state of version mismatch longer than necessary.

Example

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

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

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

2 entries were displayed.

11. Wait at least 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 might take longer than 8 minutes, depending on the characteristics of the client applications.

12. Return the aggregates to the partner node:

   `storage failover giveback -ofnode nodenameB`

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

13. Verify that all aggregates have been returned:

   `storage failover show-giveback`

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

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

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

   "Clustered Data ONTAP 8.3 High-Availability Configuration Guide"

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

   c. Reenter the `storage failover giveback` command.

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

15. Wait at least 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 might take longer than 8 minutes, depending on the characteristics of the client applications.

16. Verify that the upgrade was 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 `complete`, 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`

17. Revert the LIFs back to the node:

   `network interface revert *`

   This command returns the LIFs that were migrated away from the node.
18. Verify that the node's ports and LIFs are up and operational:
   a. Verify that the node's ports are up:

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

   If you are upgrading from the Data ONTAP 8.2 release family, you must enter this command on a node that has been upgraded to Data ONTAP 8.3.

   **Example**

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

   ```bash
   cluster1::> network port show -node node1
   Speed (Mbps) Node Port IPspace Broadcast Domain Link MTU Admin/Oper
   ------ --------- ------------ ---------------- ----- ------- ------------
   node1 e0M Default - up 1500 auto/100
   e0a Default - up 1500 auto/1000
   e0b Default - up 1500 auto/1000
   e1a Cluster Cluster up 9000 auto/10000
   e1b Cluster Cluster up 9000 auto/10000
   5 entries were displayed.
   ```

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

   ```bash
   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 their operational status is up:

   ```bash
   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 data001 up/up 192.0.2.120/24 node1 e0a true
   data002 up/up 192.0.2.121/24 node1 e0b true
   data003 up/up 192.0.2.122/24 node1 e0b true
   data004 up/up 192.0.2.123/24 node1 e0a true
   4 entries were displayed.
   ```

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

   ```bash
   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:

   ```bash
   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
   ```

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

   ```bash
   autosupport invoke -node * -type all -message "Finishing_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.

21. Confirm that the new Data ONTAP 8.3.x software is running on both nodes of the HA pair:

   system node image show

   **Example**

   This example shows version 8.3.1 as the current version on both nodes:

   ```
   cluster1::> system node image show
   Is  Is                Install
   Node  Image   Default Current Version    Date
   -------- ------- ------- ------- --------- -------------------
   node0  image1  false   false   8.2.1     5/10/2014 12:36:46
   node1  image2  true    true    8.3.1     6/25/2015 12:58:24
   node0  image2  true    true    8.3.1     6/25/2015 12:58:24
   node1  image1  false   false   8.2.1     5/10/2014 12:37:22
   4 entries were displayed.
   ```

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

   storage failover modify -node nodenameA -auto-giveback true

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

   You should do this before upgrading any additional HA pairs.

**After you finish**

Upgrade any additional HA pairs.

### Upgrading a Data ONTAP cluster nondisruptively by using the batch method

The batch upgrade method enables you to nondisruptively upgrade a cluster of eight or more nodes in a shorter amount of time than a rolling upgrade. This method involves 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**

- The cluster must be running Data ONTAP 8.3.
  - If you are upgrading from Data ONTAP 8.2, you must perform a rolling upgrade.
- You must have completed the upgrade preparation requirements and changed the default boot image.
- You must have determined the upgrade sequence for the batch upgrade.

**About this task**

**Attention**: Do not attempt to perform a batch upgrade by rebooting half of the nodes and then rebooting their high-availability partners. If you do, the cluster will lose quorum and stop serving data.

**Steps**

1. **Upgrading the first set of nodes in a batch of HA pairs** on page 74

   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 79
   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. Repeat Steps 1-2 to upgrade the second batch.

**After you finish**
You should complete post-upgrade tasks.

**Related tasks**

**Planning the upgrade sequence for a batch upgrade** on page 29
If you intend to perform a nondisruptive batch upgrade, you should plan the upgrade sequence before you upgrade Data ONTAP. By following the required sequence, you can ensure that the cluster remains up and continues serving data while you perform the NDU.

**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. If this is the first set of nodes to be upgraded, trigger an AutoSupport notification:
   
   ```bash
   autosupport invoke -node * -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.

2. For each node in the first set, set the Data ONTAP 8.3 software image to be the default image:
   
   ```bash
   system image modify {-node nodename -iscurrent false} -isdefault true
   ```
   This command uses an extended query to change the Data ONTAP 8.3 software image (which is installed as the alternate image) to be the default image for the node.

3. Verify that the Data ONTAP 8.3 software image is set as the default image:
   
   ```bash
   system image show
   ```

**Example**
This example shows that the target version is set as the default image on each of the nodes in the first set:

<table>
<thead>
<tr>
<th>Node</th>
<th>Image</th>
<th>Is Default</th>
<th>Current Version</th>
<th>Install Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>image1</td>
<td>false</td>
<td>8.3.x</td>
<td>5/10/2014 12:36:46</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>8/27/2014 12:58:24</td>
</tr>
<tr>
<td>node1</td>
<td>image1</td>
<td>true</td>
<td>false</td>
<td>5/10/2014 12:37:22</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>8/27/2014 12:59:26</td>
</tr>
<tr>
<td>node2</td>
<td>image1</td>
<td>false</td>
<td>true</td>
<td>8/27/2014 12:58:24</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>false</td>
<td>false</td>
<td>8/27/2014 12:58:24</td>
</tr>
<tr>
<td>node3</td>
<td>image1</td>
<td>true</td>
<td>false</td>
<td>8/27/2014 12:58:24</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>8/27/2014 12:58:24</td>
</tr>
<tr>
<td>node4</td>
<td>image1</td>
<td>true</td>
<td>false</td>
<td>8/27/2014 12:58:24</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>8/27/2014 12:58:24</td>
</tr>
<tr>
<td>node5</td>
<td>image1</td>
<td>true</td>
<td>false</td>
<td>8/27/2014 12:58:24</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>8/27/2014 12:58:24</td>
</tr>
</tbody>
</table>
4. For each node in the first set, disable automatic giveback on the nodes' high-availability partners by entering the following command on each node:

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

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

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

**Example**

This example shows that automatic giveback has been disabled on all of the high-availability partner nodes in the batch:

```
cluster1::> storage failover show -fields auto-giveback
node     auto-giveback
-------- ---------------
node0    true
node1    false
node2    true
node3    false
node4    true
node5    false
node6    true
node7    true
node8    true
node9    true
node10   true
node11   true
12 entries were displayed.
```

6. Determine whether the nodes to be upgraded are currently serving any clients by entering the following command twice for each node:

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

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

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

**Example**

This example shows a node with NFS, CIFS, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.
7. 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 takes 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 broadcast domain, you can migrate the LIFs to any other node that remains 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.

8. 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}
```

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

**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 partner_node}
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Is Port Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>lif1</td>
<td>up/up</td>
<td>192.0.2.130/24</td>
<td>node1</td>
<td>e0b</td>
</tr>
<tr>
<td></td>
<td>lif2</td>
<td>up/up</td>
<td>192.0.2.131/24</td>
<td>node1</td>
<td>e0b</td>
</tr>
<tr>
<td></td>
<td>lif3</td>
<td>up/up</td>
<td>192.0.2.132/24</td>
<td>node1</td>
<td>e0b</td>
</tr>
<tr>
<td>vs1</td>
<td>lif1</td>
<td>up/up</td>
<td>192.0.2.133/24</td>
<td>node1</td>
<td>e0b</td>
</tr>
<tr>
<td></td>
<td>lif2</td>
<td>up/up</td>
<td>192.0.2.134/24</td>
<td>node1</td>
<td>e0b</td>
</tr>
</tbody>
</table>

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

```
storage failover takeover {--ofnode nodename}
```

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

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.

10. 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 the In takeover state.
11. Wait at least 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 might take longer than 8 minutes depending on the characteristics of the client applications.

12. Return the aggregates to the nodes by entering the following command for each of the nodes’ partners:

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

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

13. Verify that all aggregates have been returned:

   ```
   storage failover show-giveback
   ```

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

14. If any aggregates have not been returned, do the following:
   a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.

   Clustered Data ONTAP 8.3 High-Availability Configuration Guide

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

   c. Reenter the `storage failover giveback` command.
     If you decided to override the “veto” condition, set the `-override-vetoes` parameter to `true`.

15. Wait at least 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 might take longer than 8 minutes depending on the characteristics of the client applications.

16. Verify that the upgrade was 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 complete 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
```

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

```
network interface revert *
```

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

Example

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

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

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

```
network port show -node nodename
```

Example

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

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

Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- ------------
node0
    e0M       Default      -                up       1500  auto/100
    e0a       Default      -                up       1500  auto/1000
    e0b       Default      -                up       1500  auto/1000
    e1a       Cluster      Cluster          up       9000  auto/10000
    e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

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

Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
vs0
  data001      up/up    192.0.2.120/24     node0         e0a     true
  data002      up/up    192.0.2.120/24     node0         e0b     true
  data003      up/up    192.0.2.120/24     node0         e0b     true
  data004      up/up    192.0.2.120/24     node0         e0a     true
4 entries were displayed.
```
19. 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
```

20. If you disabled automatic giveback on the high-availability partner nodes, reenable it:

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

**After you finish**

You should proceed to upgrade the nodes' HA partners as quickly as possible. If you must suspend the upgrade process for any reason, both nodes in the HA pairs should be running the same Data ONTAP version.

**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. For each of the partner nodes, set the Data ONTAP 8.3 software image to be the default image:

```
system image modify -node nodename -iscurrent false -isdefault true
```

This command uses an extended query to change the Data ONTAP 8.3 software image (which is installed as the alternate image) to be the default image for the node.

2. Verify that the Data ONTAP 8.3 software image is set as the default image:

```
system image show
```

**Example**

This example shows that the target version is set as the default image for each of the partner nodes in the first batch:

```
cluster1::> system image show
Is      Is                Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------- -------------------
node0    image1  false   false   8.3.x     5/10/2014 12:36:46
         image2  true    true    8.3.y     8/27/2014 12:58:24
node1    image1  false   true    8.3.x     5/10/2014 12:37:22
         image2  true    false   8.3.y     8/27/2014 12:59:26
node2    image1  false   false   8.3.x     5/10/2014 12:36:46
         image2  true    true    8.3.y     8/27/2014 12:58:24
node3    image1  false   true    8.3.x     5/10/2014 12:36:46
         image2  true    false   8.3.y     8/27/2014 12:58:24
node4    image1  false   false   8.3.x     5/10/2014 12:36:46
         image2  true    true    8.3.y     8/27/2014 12:58:24
node5    image1  false   true    8.3.x     5/10/2014 12:36:46
         image2  true    false   8.3.y     8/27/2014 12:58:24
node6    image1  true    true    8.3.x     5/10/2014 12:36:46
         image2  false   false   8.3.y     8/27/2014 12:58:24
node7
```
3. For each node in the second set, disable automatic giveback on the nodes' high-availability partners by entering the following command on each node:

   storage failover modify -node nodename -auto-giveback false

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

   storage failover show -fields auto-giveback

   **Example**

   This example shows that automatic giveback has been disabled on all of the high-availability partner nodes in the batch:

   ```
   cluster1::> storage failover show -fields auto-giveback
   node     auto-giveback
   -------- -------------
   node0    false
   node1    true
   node2    false
   node3    true
   node4    false
   node5    true
   node6    true
   node7    true
   node8    true
   node9    true
   node10   true
   node11   true
   12 entries were displayed.
   ```

5. 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 that the node has performed for NFS, CIFS, FC, and iSCSI clients since the node was last booted. For each protocol, you need to run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

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

   **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 8000000600 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
   ```
6. Migrate LIFs away from the nodes that will be taken over by entering the following command for each node in the partner 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 takes 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 broadcast domain, you can migrate the LIFs to any other node that remains 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.

7. 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
```

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

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

8. Initiate a takeover by entering the following command for each node in the partner set:

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

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

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.

9. Verify that the takeover was successful:

```
storage failover show
```

If you are performing a major upgrade, with one set of nodes running the newer version of Data ONTAP and their partners running an earlier Data ONTAP release family, the nodes are in a state of version mismatch. This means that normal high-availability functions such as NVRAM mirroring and automatic takeover are not in effect. You might see error messages indicating version mismatch and mailbox format problems. This is expected behavior; it represents a temporary state in a major nondisruptive upgrade and is not harmful. You should complete the upgrade procedure as quickly as possible; do not allow the nodes to remain in a state of version mismatch longer than necessary.
Example

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

```
cluster1::> storage failover show
Takeover                Possible State Description
Node           Partner        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 node8
node9          node8          true     Connected to node8
node10         node11         true     Connected to node11
node11         node10         true     Connected to node10
12 entries were displayed.
```

10. Wait at least 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 might take longer than 8 minutes depending on the characteristics of the client applications.

11. Return the aggregates to the nodes by entering the following command for each of the nodes’ partners:

   `storage failover giveback -ofnode nodename`

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

12. Verify that all aggregates have been returned:

   `storage failover show-giveback`

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

13. If any aggregates have not been returned, do the following:
   a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.

   *Clustered Data ONTAP 8.3 High-Availability Configuration Guide*

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

   c. Reenter the `storage failover giveback` command.

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

14. Wait at least 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 might take longer than 8 minutes depending on the characteristics of the client applications.
15. Verify that the upgrade was completed successfully for the nodes in the partner set:
   a. Set the privilege level to advanced:
      ```
      set -privilege advanced
      ```
   b. Ensure that upgrade status is complete for each node in the partner set:
      ```
      system node upgrade-revert show -node nodename
      ```
      The status should be listed as complete.
      If the status is not complete 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
      ```

16. Revert the LIFs back to the partner set of nodes:
    ```
    network interface revert *
    ```
    This command returns the LIFs that were migrated away from the nodes.

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

17. Verify that the nodes' ports and LIFs are up and operational by completing the following steps for each node that was upgraded:
   a. Verify that the ports are up for each node:
      ```
      network port show -node nodename
      ```
      **Example**
      ```
      This example shows that all of a node's ports are up:
      ```
      ```
      cluster1::> network port show -node node1
      Speed (Mbps)   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
      -------------------- --------- ------------ ---------------- ----- ------- -----------
      node1
      e0M       Default      -                up       1500  auto/1000
      e0a       Default      -                up       1500  auto/1000
      e0b       Default      -                up       1500  auto/1000
      e1a       Cluster      Cluster          up       9000  auto/10000
      e1b       Cluster      Cluster          up       9000  auto/10000
      5 entries were displayed.
      ```
   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
      Logical    Status     Network            Current       Current Is
      Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
      -------------- --------- -------------- ----------------- ------------- ------- ----
      vs0          data001    up/up           192.0.2.120/24  node0         e0a     true
      ```
18. 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
```

19. If this was the last set of nodes to be upgraded, trigger an AutoSupport notification:

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

This AutoSupport notification includes a record of the system status just prior to 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.

20. Confirm that the new Data ONTAP 8.3.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 8.3.0 as the current version on the first batch of nodes (node0 - node5):

<table>
<thead>
<tr>
<th>Node</th>
<th>Is Default</th>
<th>Current Version</th>
<th>Install Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>true</td>
<td>8.3.0</td>
<td>8/27/2014 13:52:22</td>
</tr>
<tr>
<td>node1</td>
<td>false</td>
<td>8.2.1</td>
<td>5/10/2014 12:37:36</td>
</tr>
<tr>
<td>node2</td>
<td>true</td>
<td>8.3.0</td>
<td>8/27/2014 13:52:22</td>
</tr>
<tr>
<td>node3</td>
<td>false</td>
<td>8.2.1</td>
<td>5/10/2014 12:37:36</td>
</tr>
<tr>
<td>node4</td>
<td>true</td>
<td>8.3.0</td>
<td>8/27/2014 13:52:22</td>
</tr>
<tr>
<td>node5</td>
<td>false</td>
<td>8.2.1</td>
<td>5/10/2014 12:37:36</td>
</tr>
<tr>
<td>node6</td>
<td>true</td>
<td>8.3.0</td>
<td>8/27/2014 13:52:22</td>
</tr>
<tr>
<td>node7</td>
<td>false</td>
<td>8.2.1</td>
<td>5/10/2014 12:37:36</td>
</tr>
<tr>
<td>node8</td>
<td>true</td>
<td>8.3.0</td>
<td>8/27/2014 13:52:22</td>
</tr>
<tr>
<td>node9</td>
<td>false</td>
<td>8.2.1</td>
<td>5/10/2014 12:37:36</td>
</tr>
<tr>
<td>node10</td>
<td>false</td>
<td>8.3.0</td>
<td>8/27/2014 13:52:22</td>
</tr>
</tbody>
</table>

84 | Upgrade and Revert/Downgrade Guide
21. If you disabled automatic giveback on the high-availability partner nodes, reenable it:

    storage failover modify -node nodename -auto-giveback true

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

    You should do this before upgrading the second batch of nodes.

### Upgrading a Data ONTAP cluster nondisruptively by using the automated method (minor NDU only)

The automated NDU method validates the cluster components to ensure that the cluster can be upgraded nondisruptively, installs the target Data ONTAP image on each node, and then, based on the number of nodes in the cluster, executes either a rolling or batch upgrade in the background.

#### Before you begin

- You must have satisfied upgrade preparation requirements.
- The cluster must be running Data ONTAP 8.3.
- For each HA pair, each node should have one or more ports on the same broadcast domain.

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

#### Steps

1. If you do not plan to monitor the progress of the upgrade process, use the `event route add-destinations` command to send a notification if the upgrade encounters an error and requires manual intervention.

    Find more information about configuring the Event Management System.

    **Example**

    In this example, if the upgrade pauses due to an error, a notification will be sent to the “test_dest” event destination.

    ```
    cluster1::> event route add-destinations -messagename upgrademgr.update.pausedErr -destinations test_dest
    ```

2. Download the target Data ONTAP software package:

    `cluster image package get -url location`

    The software package contains the target Data ONTAP image and firmware, and the set of upgrade validation rules. This package is downloaded to the cluster package repository on the root volume of one of the nodes in the cluster.

    **Example**

    ```
    cluster1::> cluster image package get -url http://www.example.com/software/8.3/image.tgz
    Software get http://www.example.com/software/8.3/image.tgz started on node node0
    Downloading package. This may take up to 10 minutes.
    ```
3. Verify that the software package is available in the cluster package repository:

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

**Example**

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
8.3.1            6/25/2015 10:32:15
```

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

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

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

You can proceed to the next step after completing all identified required actions.

**Example**

```
cluster1::> cluster image validate -version 8.3.1
It can take several minutes to complete validation...
Pre-update Check      Status      Error-Action
---------------------  ---------   -------------------------------------------
Aggregate status      OK
CIFS status           OK
Cluster health        OK
Disk status           OK
High Availability     OK
status
Disk status           OK
LIF status            OK
LIFs on home node     OK
MetroCluster          OK
configuration status
SnapMirror status     OK
Volume status         OK
mgmt epoch status     OK
mgmt RDB ring status  OK
vifmgr epoch status   OK
vifmgr RDB ring       OK
status
vldb epoch status     OK
vldb RDB ring status  OK
Overall Status        OK
17 entries were displayed.
```

5. Optional: If desired, generate a software upgrade estimate:

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

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

6. Perform the software upgrade:

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

<table>
<thead>
<tr>
<th>Upgrade and Revert/Downgrade Guide</th>
<th>98% downloaded</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no update/install in progress</td>
<td>Status of most recent operation:</td>
</tr>
<tr>
<td>Run Status: Working</td>
<td>Exit Status: Success</td>
</tr>
<tr>
<td>Phase: Download</td>
<td>Exit Message: Processing Package.</td>
</tr>
<tr>
<td>Process package Complete</td>
<td></td>
</tr>
</tbody>
</table>
This command validates that each cluster component is ready to be upgraded, installs the target Data ONTAP image on each node in the cluster, and then performs a nondisruptive upgrade in the background. If an issue is encountered, the update pauses and prompts you to take corrective action. You can use the `cluster image show-update-progress` command to view details about the issue. After correcting the issue, you can resume the update by using the `cluster image resume-update` command.

If the cluster consists of 2 through 6 nodes, a rolling upgrade is performed.

If the cluster consists of 8 or more nodes, a batch upgrade is performed by default. If desired, you can use the `-force-rolling` parameter to specify a rolling upgrade instead.

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

**Example**

```
cluster1::> cluster image update -version 8.3.1
Starting validation for this update. Please wait..
It can take several minutes to complete validation...
Non-Disruptive Check          Status   Error-Action
----------------------------- ------   -------------------------------------------
Aggregate status              OK      
CIFS status                   OK      
Cluster health status         OK      
Disk status                   OK      
High Availability status      OK      
LIF status                    OK      
LIFs on home node             OK      
MetroCluster configuration status OK      
SnapMirror status             OK      
Volume status                 OK      
mgmt epoch status             OK      
mgmt RDB ring status          OK      
vifmgr epoch status           OK      
vifmgr RDB ring status        OK      
status                        OK      
vldb epoch status             OK      
vldb RDB ring status          OK      
Overall Status                OK      
17 entries were displayed.
Would you like to proceed with update ? {y|n}: y
Starting update...
```

7. Optional: If necessary, manage the upgrade process:

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor the status and estimated duration of the upgrade</td>
<td><code>cluster image show-update-progress</code></td>
</tr>
<tr>
<td>View the log of each task that has executed during the upgrade</td>
<td><code>cluster image show-update-log</code></td>
</tr>
<tr>
<td>Pause the upgrade</td>
<td><code>cluster image pause-update</code></td>
</tr>
<tr>
<td>Resume a paused upgrade</td>
<td><code>cluster image resume-update</code></td>
</tr>
</tbody>
</table>
2. Display the cluster update history to verify that the upgrade was completed successfully for each node:

   `cluster image show-update-history`

**Example**

The Data ONTAP version numbers in the following example are provided for example purposes only:

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Package</th>
<th>Start</th>
<th>Completion</th>
<th>Component ID</th>
<th>Previous</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>8.3.y</td>
<td>11/18/2014</td>
<td>11/18/2014</td>
<td>node0</td>
<td>8.3.x</td>
<td>8.3.y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15:20:51</td>
<td>15:44:13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8.3.y</td>
<td>11/18/2014</td>
<td>11/18/2014</td>
<td>node1</td>
<td>8.3.x</td>
<td>8.3.y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15:20:51</td>
<td>16:03:20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2 entries were displayed.
```

**Related information**

*Clustered Data ONTAP 8.3 Commands: Manual Page Reference*

**Upgrading a Data ONTAP cluster nondisruptively by using OnCommand System Manager**

If you are upgrading from Data ONTAP 8.3.1 or later and you prefer a graphic interface, you can use OnCommand System Manager to perform an automated, nondisruptive upgrade.

**Before you begin**

You must have satisfied upgrade preparation requirements.

**About this task**

If you are currently running a Data ONTAP release prior to 8.3.1, you cannot use OnCommand System Manager to upgrade the cluster. You should perform a rolling or batch upgrade using the CLI.

**Steps**

1. Log in to OnCommand System Manager by using your cluster administrator credential.

   You can access OnCommand System Manager by pointing your web browser to the IP address of the cluster management LIF.

2. Expand the **Cluster** hierarchy in the left navigation pane.

3. In the navigation pane, click **Cluster Update**.

4. Follow the steps in the **Cluster Update** wizard to perform the upgrade.

   The Cluster Update wizard installs the target Data ONTAP image on each node, validates the cluster components to ensure that the cluster can be upgraded nondisruptively, and then, based on the number of nodes in the cluster, executes either a rolling or batch upgrade in the background.
After you finish
You should complete post-upgrade tasks.

Upgrading or downgrading Data ONTAP nondisruptively for a two-node MetroCluster configuration

You can upgrade or downgrade Data ONTAP nondisruptively for a two-node MetroCluster configuration. This method has several steps: initiating a negotiated switchover, updating the cluster at the “failed” site, initiating switchback, and then repeating the process on the cluster at the other site.

Before you begin
You must have satisfied upgrade or downgrade preparation requirements.

About this task
Two-node MetroCluster configurations do not have local HA pairs. Therefore, this procedure describes how to upgrade Data ONTAP nondisruptively by using the negotiated switchover and switchback operations. If you have a four-node MetroCluster configuration, which does have local HA pairs, do not use this procedure. Instead, you should use either the rolling upgrade method or the automated upgrade method to upgrade Data ONTAP nondisruptively.

Steps
1. On the cluster to be upgraded, install the new Data ONTAP software image as the default:
   
   ```system node image update -package package_location```

   **Example**
   ```
   cluster_B::> system node image update -package http://www.example.com/NewImage.tgz
   ```
   
2. Verify that the target software image is set as the default image:
   ```system node image show```

   **Example**
   ```
   cluster_B::> system node image show
   Is Is Is
   Node Image Default Current Version Install Date
   ------- ------- ------- ------- -------------------------
   node_B_1 image1 false false 8.3.x 6/18/2015 09:47:32
   image2 true true 8.3.y 6/25/2015 18:45:56
   2 entries were displayed.
   ```

3. On the cluster that is not being upgraded, initiate a negotiated switchover:
   ```metrocluster switchover```

   The operation can take several minutes. You can use the `metrocluster operation show` command to verify that the switchover is completed properly.

   **Example**
   In this example, a negotiated switchover is performed on the remote cluster (“cluster_A”). This causes the local cluster (“cluster_B”) to halt so that you can upgrade it.
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the data
Vservers on cluster "cluster_B" and
automatically re-start them on cluster
"cluster_A". It will finally gracefully shutdown
cluster "cluster_B".
Do you want to continue? {y|n}: y

4. Resynchronize the data aggregates on the “surviving” cluster:

   
   metrocluster heal -phase aggregates

   
   Example

   cluster_A::> metrocluster heal -phase aggregates
   [Job 130] Job succeeded: Heal Aggregates is successful.

5. Verify that the healing operation was completed successfully:

   
   metrocluster operation show

   
   Example

   cluster_A::> metrocluster operation show
   Operation: heal-aggregates
   State: successful
   End Time: 6/25/2015 18:45:56
   Errors: -

6. Resynchronize the root aggregates on the “surviving” cluster:

   
   metrocluster heal -phase root-aggregates

   
   Example

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

7. Verify that the healing operation was completed successfully:

   
   metrocluster operation show

   
   Example

   cluster_A::> metrocluster operation show
   Operation: heal-root-aggregates
   State: successful
   Start Time: 6/25/2015 18:47:03
   Errors: -

8. On the upgraded cluster, boot the node from the LOADER prompt:

   
   boot_ontap

9. Wait for the boot process to finish, and then perform a switchback from the “surviving” cluster:

   
   metrocluster switchback

10. Verify that the switchback was completed successfully:

    
    metrocluster operation show
11. Repeat Steps 1 on page 89 through 10 on page 90 on the other cluster.

12. Verify that the MetroCluster configuration is healthy:
   a. Check the configuration:
      
      \texttt{metrocluster check run}

      \textbf{Example}
      
      \begin{verbatim}
      cluster_A::> metrocluster check run
      Last Checked On: 6/10/2015 17:10:33
      Component           Result
      ------------------- ---------
      nodes               ok
      lifs                ok
      config-replication  ok
      aggregates          ok
      4 entries were displayed.
      Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.
      To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.
      \end{verbatim}

   b. Display more detailed results from the \texttt{metrocluster check run} command:
      
      \begin{verbatim}
      metrocluster check aggregate show
      metrocluster check config-replication show
      metrocluster check lif show
      metrocluster check node show
      \end{verbatim}

   c. Set the privilege level to advanced:
      
      \begin{verbatim}
      set -privilege advanced
      \end{verbatim}

   d. Simulate the switchover operation:
      
      \begin{verbatim}
      metrocluster switchover -simulate
      \end{verbatim}

   e. Review the results of the switchover simulation:
      
      \begin{verbatim}
      metrocluster operation show
      \end{verbatim}

      \textbf{Example}
      
      \begin{verbatim}
      cluster_A::*> metrocluster operation show
      Operation: switchover
      State: successful
      Errors: -
      \end{verbatim}

   f. Return to the admin privilege level:
      
      \begin{verbatim}
      set -privilege admin
      \end{verbatim}
g. Repeat Steps 12.a through 12.f on the other cluster.

After you finish
You should perform any post-upgrade or post-downgrade tasks.

Related information
Clustered Data ONTAP 8.3 MetroCluster Management and Disaster Recovery Guide

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, rebooting each node in the cluster, and then reenabling storage failover.

Before you begin
• You must have satisfied upgrade preparation requirements.
• If you are operating in a SAN environment, all SAN clients must be shut down or suspended until the upgrade is complete.
  If SAN clients are not shut down or suspended prior to a disruptive upgrade, the client file systems and applications will suffer errors that might require manual recovery after the upgrade is completed.
• If you want to upgrade the nodes in batches, you must have determined the upgrade sequence.
  You can only upgrade nodes in batches if you are performing a minor upgrade within the Data ONTAP 8.3 release family, and if the cluster consists of at least eight nodes.

About this task
In a disruptive upgrade, downtime is required because storage failover is disabled for each HA pair, and each node is updated. When storage failover is disabled, each node behaves as a single-node cluster; that is, system services associated with the node are interrupted for as long as it takes the system to reboot.

Steps
1. Set the Data ONTAP 8.3 software image to be the default image:
   
   system image modify (-node * -iscurrent false) -isdefault true

   This command uses an extended query to change the Data ONTAP 8.3 software image (which is installed as the alternate image) to be the default image for each node.

2. Verify that the Data ONTAP 8.3 software image is set as the default image:
   
   system image show

Example
This example shows that version 8.3.1 is set as the default image on both nodes:

```
cluster1::> system image show

<table>
<thead>
<tr>
<th>Node</th>
<th>Is</th>
<th>Is</th>
<th>Install</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>image1</td>
<td>false  true</td>
<td>8.2.1 5/10/2014 12:36:46</td>
</tr>
<tr>
<td></td>
<td>image2</td>
<td>true  false</td>
<td>8.3.1 6/25/2015 12:58:24</td>
</tr>
</tbody>
</table>
```
3. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If the cluster consists of...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>One node</td>
<td>Continue to the next step.</td>
</tr>
</tbody>
</table>
| Two nodes                   | a. Disable cluster high availability:
                                  
                                  `cluster ha modify -configured false`
                                  
                                  b. Disable storage failover for the HA pair:
                                  
                                  `storage failover modify -node * -enabled false` |
| More than two nodes          | Disable storage failover for each HA pair in the cluster:
                                  
                                  `storage failover modify -node * -enabled false` |

4. Reboot one or more nodes.

<table>
<thead>
<tr>
<th>If the cluster consists of...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| Fewer than eight nodes, or you are performing a major upgrade | Reboot a node in the cluster:
                                  
                                  `system node reboot -node nodename`
                                  
                                  **Attention:** Do not reboot more than one node at a time. |
| Eight or more nodes, and you are performing a minor upgrade | Reboot each node in the set:
                                  
                                  `system node reboot -node nodename`
                                  
                                  You must follow the batch upgrade sequence guidelines to determine which nodes can be rebooted concurrently. |

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

5. After the node or set of nodes have rebooted with the new Data ONTAP image, confirm that the new software is running:

`system node image show`

**Example**

This example shows that Data ONTAP 8.3.1 is the current version on node0:

```
node0
  image1 true true 8.3.1 6/25/2015 13:52:22
  image2 false false 8.2.1 5/10/2014 12:37:36
4 entries were displayed.
```

6. Verify that the upgrade was completed successfully:

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 upgrade is not successful, from the node, run the `system node upgrade-revert` 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
```

7. Repeat Steps 4 through 6 for each additional node.

8. If the cluster consists of two or more nodes, enable storage failover for each HA pair in the cluster:

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

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

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

Related tasks

*Planning the upgrade sequence for a batch upgrade* on page 29

If you intend to perform a nondisruptive batch upgrade, you should plan the upgrade sequence before you upgrade Data ONTAP. By following the required sequence, you can ensure that the cluster remains up and continues serving data while you perform the NDU.

**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.

**Steps**

1. **Verifying the cluster version** on page 95
   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.

2. **Verifying cluster health** on page 96
   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 that the cluster is in quorum.

3. **Verifying storage health** on page 97
   Before and after you upgrade, revert, or downgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

4. **Verifying that IPv6 LIFs can connect to external servers** on page 98
   Data ONTAP 8.2.2 and earlier can only verify that each SVM can connect to its external servers through IPv4 addresses. Therefore, after upgrading to Data ONTAP 8.3, you should verify that each SVM can connect to an external server using an IPv6 address.

5. **Verifying networking and storage status for MetroCluster configurations** on page 98
   Before and after performing a minor upgrade or downgrade in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

6. **Enabling and reverting LIFs to home ports** on page 101
   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.

7. **Relocating moved load-sharing mirror source volumes** on page 102
After successfully completing a nondisruptive upgrade, you can move load-sharing mirror source volumes back to the locations they were in originally before the upgrade.

8. **Resuming SnapMirror operations** on page 102
After completing a nondisruptive upgrade or downgrade, you must resume any SnapMirror relationships that were suspended.

9. **Reenabling automatic LIF rebalancing** on page 103
If you previously disabled automatic LIF rebalancing to perform a batch upgrade, you should reenable it after completing the upgrade.

10. **Verifying the SAN configuration after an upgrade** on page 103
If you are upgrading in a SAN environment, then after the upgrade, you should verify that each initiator that was connected to a LIF before the upgrade has successfully reconnected to the LIF.

11. **Verifying NFS Kerberos configurations after upgrading** on page 103
Beginning with Data ONTAP 8.3, Data ONTAP restricts the use of identical service principal names (SPNs) for NFS Kerberos configurations when used across multiple SVMs and deletes NFS Kerberos configurations that are no longer permitted. To avoid NFS client Kerberos authentication problems after upgrading, you must check whether your system is affected by this change and reconfigure accordingly.

12. **Verifying the networking configuration after a major upgrade** on page 104
After completing a major upgrade to Data ONTAP 8.3, you should verify that the LIFs required for external server connectivity, failover groups, and broadcast domains are configured correctly for your environment.

13. **Enabling volume guarantees after the upgrade** on page 105
If your cluster included FlexVol volumes with a guarantee of file before the upgrade, and those volumes contained space-reserved LUNs or files, the volumes have a disabled guarantee after the upgrade. To provide the same guarantee to those files and LUNs, you must enable the guarantee for those volumes.

14. **Configuring LDAP clients to use TLS for highest security** on page 106
If you had previously configured LDAP clients to use LDAP over SSL/TLS for secure communications with LDAP servers, the LDAP client was able to use the less secure SSLv2 protocol. After upgrading to this release, if your environment supports it, you should disallow the use of SSLv2 to force the use of TLS for the highest level of security.

15. **Setting the desired NT ACL permissions display level for NFS clients** on page 107
After upgrading to Data ONTAP 8.3.1, the default handling for displaying NT ACL permissions to NFS clients has changed. You should check the setting and change it to the desired setting for your environment if necessary.

16. **When you need to update the Disk Qualification Package** on page 108
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.

### 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
```

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

### Verifying cluster 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 that the cluster is in quorum.

#### 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.

2. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

   Enter `y` to continue.

3. Verify the configuration details for each RDB process.

   You should verify the following configuration details:

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

   **To display this RDB process...**

   **Enter this command...**

<table>
<thead>
<tr>
<th>Management application</th>
<th><code>cluster ring show -unitname mgmt</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume location database</td>
<td><code>cluster ring show -unitname vldb</code></td>
</tr>
<tr>
<td>Virtual-Interface manager</td>
<td><code>cluster ring show -unitname vifmgr</code></td>
</tr>
<tr>
<td>SAN management daemon</td>
<td><code>cluster ring show -unitname bcomd</code></td>
</tr>
</tbody>
</table>

   **Example**

   This example shows the volume location database process:

   ```
   cluster1::*> cluster ring show -unitname vldb
   Node  UnitName Epoch  DB Epoch DB Trnxs Master    Online
         -------- --------- -------- ------- ---------- -------
   node0  vldb     154      154     14847     node0     master
   ```
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.

Example

```
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 ...
```

5. Return to the admin privilege level:

   `set -privilege admin`

Related information

*Clustered Data ONTAP 8.3 System Administration Guide*

### Verifying storage health

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

**Steps**

1. If you are preparing to upgrade, revert, or downgrade, verify disk status:

<table>
<thead>
<tr>
<th>To check for</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broken disks</td>
<td>a. Display any broken disks:</td>
</tr>
<tr>
<td></td>
<td><code>storage disk show -state broken</code></td>
</tr>
<tr>
<td></td>
<td>b. Remove or replace any broken disks.</td>
</tr>
<tr>
<td>Disks undergoing maintenance or reconstruction</td>
<td>a. Display any disks in maintenance, pending, or reconstructing states:</td>
</tr>
<tr>
<td></td>
<td>`storage disk show -state maintenance</td>
</tr>
<tr>
<td></td>
<td>b. Wait for the maintenance or reconstruction operation to finish before</td>
</tr>
<tr>
<td></td>
<td>proceeding.</td>
</tr>
</tbody>
</table>

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates:

   `storage aggregate show -state !online`

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

Example

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```
3. Verify that all volumes are online by displaying any volumes that are not online:

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

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

Example

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

Related information

- *Clustered Data ONTAP 8.3 Logical Storage Management Guide*
- *Clustered Data ONTAP 8.3 Physical Storage Management Guide*

**Verifying that IPv6 LIFs can connect to external servers**

Data ONTAP 8.2.2 and earlier can only verify that each SVM can connect to its external servers through IPv4 addresses. Therefore, after upgrading to Data ONTAP 8.3, you should verify that each SVM can connect to an external server using an IPv6 address.

**About this task**

If you upgraded from Data ONTAP 8.2.3 or later, you do not need to perform this procedure. These releases validate the IPv6 connectivity when you installed the target software image on the first node.

**Steps**

1. For each SVM, verify that its external servers are reachable from IPv6 addresses:

```
vserver check lif-multitenancy run -vserver Vserver_name
```

You can use the `-verbose` parameter (advanced privilege level) to display additional information about each connectivity test.

Example

```
cluster1::> vserver check lif-multitenancy run -vserver vs0
SUCCESS: All external servers are reachable.
```

2. Make any required networking configuration changes, and then repeat Step 1.

**Verifying networking and storage status for MetroCluster configurations**

Before and after performing a minor upgrade or downgrade in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

**About this task**

If you are performing a major upgrade from Data ONTAP 8.2, you do not need to complete this procedure.

**Steps**

1. Verify the LIF status:

```
network interface show
```

In normal operation, LIFs for source SVMs must be up and located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs should be up, but they do not need to be located on their home nodes.
<table>
<thead>
<tr>
<th>Vserver</th>
<th>Logical Interface</th>
<th>Status</th>
<th>Admin/Oper</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Port</th>
<th>Is Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1-a1_clus1</td>
<td>up/up</td>
<td>192.0.2.1/24</td>
<td>cluster1-01</td>
<td>e2a true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_clus2</td>
<td>up/up</td>
<td>192.0.2.2/24</td>
<td>cluster1-01</td>
<td>e2b true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_clus1</td>
<td>up/up</td>
<td>192.0.2.3/24</td>
<td>cluster1-02</td>
<td>e2a true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_clus2</td>
<td>up/up</td>
<td>192.0.2.4/24</td>
<td>cluster1-02</td>
<td>e2b true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_inet4_intercluster1</td>
<td>up/up</td>
<td>198.51.100.2/24</td>
<td>cluster1-01</td>
<td>e3a true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_inet4_intercluster2</td>
<td>up/up</td>
<td>198.51.100.3/24</td>
<td>cluster1-01</td>
<td>e3c true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_mgmt1</td>
<td>up/up</td>
<td>198.51.100.4/24</td>
<td>cluster1-01</td>
<td>e0M true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_data1</td>
<td>up/up</td>
<td>198.51.100.8/24</td>
<td>cluster1-01</td>
<td>e3d true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_data2</td>
<td>up/up</td>
<td>198.51.100.9/24</td>
<td>cluster1-01</td>
<td>e3d true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_data3</td>
<td>up/up</td>
<td>198.51.100.10/24</td>
<td>cluster1-01</td>
<td>e3c true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_data4</td>
<td>up/up</td>
<td>198.51.100.11/24</td>
<td>cluster1-01</td>
<td>e3a true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_data1</td>
<td>up/up</td>
<td>198.51.100.12/24</td>
<td>cluster1-01</td>
<td>e3a true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_data2</td>
<td>up/up</td>
<td>198.51.100.13/24</td>
<td>cluster1-01</td>
<td>e3a true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_data3</td>
<td>up/up</td>
<td>198.51.100.14/24</td>
<td>cluster1-01</td>
<td>e3c true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_data4</td>
<td>up/up</td>
<td>198.51.100.15/24</td>
<td>cluster1-01</td>
<td>e3c true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-b1_data1</td>
<td>up/down</td>
<td>198.51.100.16/24</td>
<td>cluster1-02</td>
<td>e3a true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-b1_data2</td>
<td>up/down</td>
<td>198.51.100.17/24</td>
<td>cluster1-02</td>
<td>e3a true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-b1_data3</td>
<td>up/down</td>
<td>198.51.100.18/24</td>
<td>cluster1-02</td>
<td>e3a true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-b1_data4</td>
<td>up/down</td>
<td>198.51.100.19/24</td>
<td>cluster1-02</td>
<td>e3b true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-b2_data1</td>
<td>up/down</td>
<td>198.51.100.20/24</td>
<td>cluster1-02</td>
<td>e3a true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-b2_data2</td>
<td>up/down</td>
<td>198.51.100.21/24</td>
<td>cluster1-02</td>
<td>e3a true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-b2_data3</td>
<td>up/down</td>
<td>198.51.100.22/24</td>
<td>cluster1-02</td>
<td>e3b true</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. Verify the state of the aggregates:

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

   This command displays any aggregates that are not online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

   **Example**

   This example shows a cluster in normal operation:

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

   **Example**

   This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are offline:

   ```shell
   cluster1::> storage aggregate show -state !online
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID Status
   --------- -------- --------- ----- ------- ------ ---------------- ------------
   aggr0_b1 0B        0B     0% offline      0 cluster2-01      raid_dp, mirror degraded
   aggr0_b2 0B        0B     0% offline      0 cluster2-02      raid_dp, mirror degraded
   2 entries were displayed.
   ```

3. Verify the state of the volumes:

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

   This command displays any volumes that are not online. In normal operation, all root and data volumes owned by the local cluster's SVMs must be online. However, if the MetroCluster configuration is in switchover, all volumes must be online.

   **Example**

   This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online:

   ```shell
   cluster1::> volume show -state !online
   Vserver   Volume       Aggregate    State      Type       Size  Available Used%
   --------- ------------ ------------ ---------- ---- ---------- ---------- ----- 
   vs2-mc    vol1         aggr1_b1     -          RW            -          -     -
   vs2-mc    root_vs2     aggr0_b1     -          RW            -          -     -
   vs2-mc    vol2         aggr1_b1     -          RW            -          -     -
   vs2-mc    vol3         aggr1_b1     -          RW            -          -     -
   vs2-mc    vol4         aggr1_b1     -          RW            -          -     -
   5 entries were displayed.
   ```
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:
   ```bash
   network interface show
   ```

   **Example**
   
   This example displays the status of all LIFs for a Storage Virtual Machine (SVM, formerly known as Vserver).
   ```bash
   cluster1::> network interface show -vserver vs0
   Logical     Status     Network            Current       Current Is
   Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
   ----------- ---------- ---------- ------------------ ------------- ------- ----
   vs0
   data001    down/down  192.0.2.120/24     node0         e0e     true
   data002    down/down  192.0.2.121/24     node0         e0f     true
   data003    down/down  192.0.2.122/24     node0         e2a     true
   data004    down/down  192.0.2.123/24     node0         e2b     true
   data005    down/down  192.0.2.124/24     node0         e0e     false
   data006    down/down  192.0.2.125/24     node0         e0f     false
   data007    down/down  192.0.2.126/24     node0         e2a     false
   data008    down/down  192.0.2.127/24     node0         e2b     false
   8 entries were displayed.
   ```

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

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

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

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

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

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

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

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

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         e0e     true
vs0          data002      up/up    192.0.2.121/24     node0         e0f     true
vs0          data003      up/up    192.0.2.122/24     node0         e2a     true
vs0          data004      up/up    192.0.2.123/24     node0         e2b     true
vs0          data005      up/up    192.0.2.124/24     node1         e0e     true
vs0          data006      up/up    192.0.2.125/24     node1         e0f     true
vs0          data007      up/up    192.0.2.126/24     node1         e2a     true
8 entries were displayed.
```

Relocating moved load-sharing mirror source volumes

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

Steps

1. Identify the location to which you are moving the load-sharing mirror source volume by using the record you created before moving the load-sharing mirror source volume.
   
   *Preparing all load-sharing mirrors for a major upgrade* on page 54

2. Move the load-sharing mirror source volume back to its original location by using the `volume move start` command.

Resuming SnapMirror operations

After completing a nondisruptive upgrade 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 *`
   
   This command resumes the transfers for all quiesced SnapMirror relationships.

2. Verify that the SnapMirror operations have resumed:
   
   `snapmirror show`

Example

```
cluster1::> snapmirror show

Source Path Type                      Destination Path Type                  Mirror State     Relationship   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
```

Relocating moved load-sharing mirror source volumes

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

Steps

1. Identify the location to which you are moving the load-sharing mirror source volume by using the record you created before moving the load-sharing mirror source volume.
   
   *Preparing all load-sharing mirrors for a major upgrade* on page 54

2. Move the load-sharing mirror source volume back to its original location by using the `volume move start` command.

Resuming SnapMirror operations

After completing a nondisruptive upgrade 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 *`
   
   This command resumes the transfers for all quiesced SnapMirror relationships.

2. Verify that the SnapMirror operations have resumed:
   
   `snapmirror show`

Example

```
cluster1::> snapmirror show

Source Path Type                      Destination Path Type                  Mirror State     Relationship   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
```
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.

**Reenabling 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:
   ```bash
   set -privilege advanced
   ```
2. Reenable automatic LIF rebalancing for each LIF as needed:
   ```bash
   network interface modify -vserver Vserver_name -lif LIF_name -allow-lb-migrate true
   ```
3. Return to the admin privilege level:
   ```bash
   set -privilege admin
   ```

**Verifying the SAN configuration after an upgrade**

If you are upgrading in a SAN environment, then after the upgrade, you should verify that each initiator that was connected to a LIF before the upgrade has successfully reconnected to the LIF.

**Step**

1. Verify that each initiator is connected to the correct LIF.
   
   You should compare the list of initiators to the list you made during the upgrade preparation.

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

**Verifying NFS Kerberos configurations after upgrading**

Beginning with Data ONTAP 8.3, Data ONTAP restricts the use of identical service principal names (SPNs) for NFS Kerberos configurations when used across multiple SVMs and deletes NFS Kerberos configurations that are no longer permitted. To avoid NFS client Kerberos authentication problems
after upgrading, you must check whether your system is affected by this change and reconfigure accordingly.

**About this task**

In previous releases, Data ONTAP allowed multiple SVMs to share NFS Kerberos credentials for LIFs across multiple SVMs. This configuration is no longer allowed in Data ONTAP 8.3. If your system currently uses SPNs in a way that allows credential (KDC accounts and keys) sharing across multiple SVMs, Data ONTAP automatically disables NFS Kerberos on all such LIFs after upgrading.

When a node running Data ONTAP 8.3 reboots, it examines all existing NFS Kerberos configurations across all SVMs. If any LIF of one SVM shares the NFS Kerberos credential with a LIF on another SVM, Data ONTAP disables NFS Kerberos on both LIFs and creates an EMS message. The EMS message enables you to identify each LIF for which you need to reconfigure NFS Kerberos.

**Steps**

1. Check your EMS log for messages indicating which NFS Kerberos configurations were disabled.
2. In the EMS messages, identify each LIF whose NFS Kerberos configuration was disabled.
3. For each LIF, reconfigure NFS Kerberos by using the `vserver nfs kerberos interface enable` command.

   You must create the new NFS Kerberos configuration with new separate SPNs to regain NFS Kerberos functionality for those SVMs.

**Verifying the networking configuration after a major upgrade**

After completing a major upgrade to Data ONTAP 8.3, you should verify that the LIFs required for external server connectivity, failover groups, and broadcast domains are configured correctly for your environment.

**About this task**

In Data ONTAP 8.3, an SVM can connect to its external servers through any of its data LIFs regardless of which node hosts the LIF. Therefore, you should keep the data LIFs that you configured during the upgrade preparation to ensure that each SVM can reach each of its external servers.

However, you can modify these LIFs to be located on any node in the cluster, and to not automatically revert.

**Steps**

1. Verify the broadcast domains:

   `network port broadcast-domain show`

   During the upgrade to the Data ONTAP 8.3 release family, Data ONTAP automatically creates broadcast domains based on the failover groups in the cluster. For each layer 2 network, you should verify that a broadcast domain exists, and that it includes all of the ports that belong to the network. If you need to make any changes, you can use the `network port broadcast-domain` commands.

**Example**

```
cluster1::> network port broadcast-domain show
IPspace Broadcast
Name      Domain Name MTU    Port List     Status Details
--------    ----------- ---- --------------------- --------------
Cluster     Cluster     9000 node0:e0a       complete
            Cluster     node0:e0b       complete
```
2. If necessary, use the network interface modify command to change the LIFs that you configured for external server connectivity.

<table>
<thead>
<tr>
<th>To...</th>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move the LIF to a different home node or port</td>
<td>a. Change the LIF’s home node or port:</td>
</tr>
<tr>
<td></td>
<td>network interface modify -vserver Vserver_name -lif LIF_name -home-node node_name -home-port port</td>
</tr>
<tr>
<td></td>
<td>b. Revert the LIF to the new home node or port:</td>
</tr>
<tr>
<td></td>
<td>network interface revert -vserver Vserver_name -lif LIF_name</td>
</tr>
<tr>
<td></td>
<td>The LIFs required for external server connectivity must be located on the first node for the duration of the upgrade. However, these LIFs can be located on any node after the upgrade is complete.</td>
</tr>
<tr>
<td>Set the LIF not to revert automatically</td>
<td>network interface modify -vserver Vserver_name -lif LIF_name -auto-revert false</td>
</tr>
<tr>
<td></td>
<td>The LIFs required for external server connectivity must be set to automatically revert for the duration of the upgrade. However, this setting is no longer required after the upgrade is complete.</td>
</tr>
<tr>
<td>Change the LIF to use any of the ports in its broadcast domain</td>
<td>network interface modify -vserver Vserver_name -lif LIF_name -failover-group failover_group_name -failover-policy policy</td>
</tr>
<tr>
<td></td>
<td>Before the upgrade, you created one or more failover groups consisting of ports on the first HA pair only. These failover groups were necessary to ensure that each SVM could contact its external servers during the upgrade process. However, after the upgrade is complete, the LIFs required for external server connectivity are no longer restricted to the first two nodes in the cluster; you can modify them to use any of the nodes and ports in the appropriate broadcast domains.</td>
</tr>
</tbody>
</table>

Related information

Clustered Data ONTAP 8.3 Network Management Guide

Enabling volume guarantees after the upgrade

If your cluster included FlexVol volumes with a guarantee of file before the upgrade, and those volumes contained space-reserved LUNs or files, the volumes have a disabled guarantee after the
upgrade. To provide the same guarantee to those files and LUNs, you must enable the guarantee for those volumes.

**About this task**

The volume guarantee type of *file* is not supported for Data ONTAP 8.3 and later. Volumes with a volume guarantee of *file* are converted during the upgrade according to whether they contain any space-reserved LUNs or files:

- If the volume contains no space-reserved LUNs or files, its volume guarantee is converted to none.
- If the volume contains space-reserved LUNs or files, its volume guarantee is converted to volume.

However, because there might not be enough free space available to honor the volume guarantee, the volume guarantee is initially disabled. You must enable it manually before the space-reserved LUN or file has the same space protections it had before the upgrade.

If any of the affected volumes contained free space or unreserved files before the upgrade, those volumes consume additional space from the aggregate when their guarantee is enabled.

**Steps**

1. Display the volumes with a disabled volume guarantee:
   ```
   volume show -space-guarantee volume -space-guarantee-enabled false
   ```

2. If no volumes are displayed, you are done with this task.

3. Enable the guarantees for the volumes with disabled volume guarantees:
   ```
   volume modify { -space-guarantee volume -space-guarantee-enabled false } -space-guarantee volume
   ```
   If there is sufficient free space available in the aggregate to honor the volume guarantees, the volume guarantees are enabled.

4. If there is insufficient free space in the aggregate to enable the volume guarantees, resize the volumes or add storage to the aggregate and retry the previous command.

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

If you had previously configured LDAP clients to use LDAP over SSL/TLS for secure communications with LDAP servers, the LDAP client was able to use the less secure SSLv2 protocol. After upgrading to this release, if your environment supports it, you should disallow the use of SSLv2 to force the use of TLS for the highest level of security.

**About this task**

By default, LDAP communications between client and server applications are not encrypted. You can configure Data ONTAP LDAP clients to use LDAP over SSL/TLS by enabling the `-use-start-tls` parameter. If your environment supports TLS, you should disallow the use of SSL and enforce the use of TLS.

**Steps**

1. Verify that the LDAP servers in your environment support TLS.
   - If they do not, do not proceed. You should upgrade your LDAP servers to a version that supports TLS.

2. Check which Data ONTAP LDAP client configurations have LDAP over SSL/TLS enabled:
vserver services name-service ldap client -show

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

3. For each LDAP client configuration, disallow SSL to enforce the use of TLS:
   vserver services name-service ldap client modify -vserver vserver_name -client-config ldap_client_config_name -allow-ssl false

4. Verify that the use of SSL is no longer allowed for any LDAP clients:
   vserver services name-service ldap client -show

Related information

Clustered Data ONTAP 8.3 File Access Management Guide for NFS

Setting the desired NT ACL permissions display level for NFS clients

After upgrading to Data ONTAP 8.3.1, the default handling for displaying NT ACL permissions to NFS clients has changed. You should check the setting and change it to the desired setting for your environment if necessary.

About this task

In multiprotocol environments, Data ONTAP displays to NFS clients the permissions of NTFS security-style files and directories based on the access granted by the NT ACL to any user. In previous releases of Data ONTAP, Data ONTAP by default displayed to NFS clients the permission based on the maximum access granted by the NT ACL. After upgrading to Data ONTAP 8.3.1, the default setting changes to display permissions based on the minimum access granted by the NT ACL. This change applies to new and existing Storage Virtual Machines (SVMs).

Steps

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

2. Check the setting for displaying NT ACL permissions for NFS clients:
   vserver nfs show -vserver vserver_name -fields ntacl-display-permissive-perms
   After upgrading to Data ONTAP 8.3.1, the value for this new parameter is disabled, meaning Data ONTAP displays the minimum permissions.

3. If you prefer to display the maximum permissions, change the setting individually for each SVM as desired:
   vserver nfs modify -vserver vserver_name -ntacl-display-permissive-perms enabled

4. Verify that the change took effect:
   vserver nfs show -vserver vserver_name -fields ntacl-display-permissive-perms

5. Return to the admin privilege level:
   set -privilege admin
When you need to update the Disk Qualification Package

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

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

• Whenever you add a new drive type or size to the node
  For example, if you already have 1-TB drives and add 2-TB drives, you need to check for the latest DQP update.

• Whenever you update the disk firmware

• Whenever newer disk firmware or DQP files are available

• Whenever you upgrade to a new version of Data ONTAP.
  The DQP is not updated as part of a Data ONTAP upgrade.

Related information

* NetApp Downloads: Disk Qualification Package
* NetApp Downloads: Disk Drive and Firmware
Reverting clusters to an earlier Data ONTAP release family

Transitioning a cluster to a release in an earlier Data ONTAP release family is referred to as a reversion. Reverting is always disruptive, and it requires planning, preparation, the reversion itself, and several 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.

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.

Cluster revert workflow

You can use the cluster revert workflow to plan the reversion, prepare for the reversion, perform the reversion, and complete post-reversion tasks.
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.

Steps

1. **Reviewing pre-reversion resources** on page 110
   Before upgrading Data ONTAP, you should review resources to understand issues you must resolve before upgrading, understand new system behavior in the target release, and confirm hardware support.

2. **Reviewing cluster reversion requirements** on page 111
   Before reverting Data ONTAP, you must verify that your cluster meets the general reversion requirements. Some configurations and features also have requirements that you should understand.

Reviewing pre-reversion resources

Before upgrading Data ONTAP, you should review resources to understand issues you must resolve before upgrading, understand new system behavior in the target release, and confirm hardware support.

Steps

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

   *Find the Release Notes for your version of Data ONTAP 8*

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

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

3. Confirm that your cluster and management switches are supported in the target release.
   
   You must verify that the NX-OS (cluster network switches), IOS (management network switches), and reference configuration file (RCF) software versions are compatible with the version of Data ONTAP to which you are reverting.

NetApp Downloads: Cisco Ethernet Switch

4. If your cluster is configured for SAN, confirm that the SAN configuration is fully supported.
   
   All SAN components—including target Data ONTAP software version, host OS and patches, required Host Utilities software, and adapter drivers and firmware—should be supported.

NetApp Interoperability Matrix Tool

Reviewing cluster reversion requirements

Before reverting Data ONTAP, you must verify that your cluster meets the general reversion requirements. Some configurations and features also have requirements that you should understand.

Reversion process considerations

You need to consider the revert issues and limitations before beginning a Data ONTAP reversion.

- Clusters can be reverted from Data ONTAP 8.3.x to 8.2.1 or later.
- Reversion is disruptive.
  
  No client access can occur during the reversion. If you are reverting a production cluster, be sure to include this disruption in your planning.
- Reversion affects all nodes in the cluster.
  
  The reversion affects all nodes in the cluster; however, the reversion must be performed and completed on each HA pair before other HA pairs are reverted.
- The reversion is complete when all nodes are running the new target release.
  
  When the cluster is in a mixed-version state, you should not enter any commands that alter the cluster operation or configuration except as necessary to satisfy reversion requirements; monitoring operations are permitted.

  Attention: If you cannot 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.

- When you revert a node, it clears the cached data in a Flash Cache module.
  
  Because there is no cached data in the Flash Cache module, the node serves initial read requests from disk, which results in decreased read performance during this period. The node repopulates the cache as it serves read requests.
- A LUN that is backed up to tape running on Data ONTAP 8.3 can be restored only to 8.3 and later releases and not to an earlier release.

Reversion requirements for SnapMirror and SnapVault relationships

The `system node revert-to` command notifies you of any SnapMirror and SnapVault relationships that need to be deleted or reconfigured for the reversion process to be completed. However, you should be aware of these requirements before you begin the reversion.

- All SnapVault and data protection mirror relationships must be quiesced and then broken.
  
  After the reversion is completed, you can resynchronize and resume these relationships if a common Snapshot copy exists.
SnapVault relationships must not contain the following SnapMirror policy types:

- `async-mirror`
  You must delete any relationship that uses this policy type.

- `MirrorAndVault`
  If any of these relationships exist, you should change the SnapMirror policy to `mirror-vault`.

- All load-sharing mirror relationships and destination volumes must be deleted.
- SnapMirror relationships with FlexClone destination volumes must be deleted.
- Network compression must be disabled for each SnapMirror policy.
- The `all_source_snapshot` rule must be removed from any `async-mirror` type SnapMirror policies.
- Any currently running single file and Snapshot restore operations must be completed before the reversion can proceed.
  You can either wait for the restore operation to finish, or you can abort it.
- Any incomplete single file and Snapshot restore operations must be removed by using the `snapmirror restore` command.

**Reversion considerations for an Infinite Volume**

When reverting a cluster that contains an Infinite Volume from Data ONTAP 8.3.x to Data ONTAP 8.2.x, you must plan to create a namespace mirror constituent to protect the namespace constituent and to support incremental tape backup, if configured, after you complete the reversion.

All the Infinite Volumes in a cluster running Data ONTAP 8.2 or later must have a namespace mirror constituent to provide data protection for the namespace constituent. If the Infinite Volume has SnapDiff enabled and is configured for incremental tape backup, each node that the Infinite Volume spans requires a namespace mirror constituent, except the node with the namespace constituent.

The process of reverting to Data ONTAP 8.2.x removes the namespace mirror constituents and does not automatically re-create the namespace mirror constituents for the Infinite Volume. You must plan to create the namespace mirror constituents after you complete the reversion.

Before you revert an Infinite Volume with storage classes, you should identify the name of the aggregate on the node that contains the namespace mirror constituent. If the Infinite Volume with storage classes is configured for incremental tape backup, multiple nodes contain namespace mirror constituents, and you should identify the name of the aggregate on each node that contains a namespace mirror constituent. When you create namespace mirror constituents after the reversion, you must specify the name of the aggregate for each node on which to create the namespace mirror constituent.

**Note:** This requirement applies only to an Infinite Volume that uses storage classes.

**Related tasks**

*Creating namespace mirror constituents for reverted Infinite Volumes* on page 133

After reverting a cluster that contains an Infinite Volume to Data ONTAP 8.2.x, you must create one or more namespace mirror constituents. How you create the namespace mirror constituents depends on whether the Infinite Volume uses storage classes and is configured for tape backup.
Preparing to revert Data ONTAP clusters

Before reverting to an earlier Data ONTAP release family, you must verify that the cluster is ready to be reverted and make any required configuration changes.

Steps

1. **Verifying that the cluster is ready to be reverted** on page 113
   Before you perform the reversion, you should verify that your cluster configuration is healthy.

2. **Preparing to revert production clusters** on page 116
   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.

3. **Obtaining Data ONTAP software images** on page 122
   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.

4. **Installing Data ONTAP software images for a reversion** on page 122
   Before performing a reversion to Data ONTAP 8.2, you must install the target Data ONTAP software image on each node in the cluster.

Verifying that the cluster is ready to be reverted

Before you perform the reversion, you should verify that your cluster configuration is healthy.

Verifying cluster 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 that the cluster is in quorum.

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.

2. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

   Enter `y` to continue.

3. Verify the configuration details for each RDB process.
   You should verify the following configuration details:
   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.
   Note that each ring might have a different quorum master.
To display this RDB process...

Enter this command...

<table>
<thead>
<tr>
<th>Management application</th>
<th><code>cluster ring show -unitname mgmt</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume location database</td>
<td><code>cluster ring show -unitname vldb</code></td>
</tr>
<tr>
<td>Virtual-Interface manager</td>
<td><code>cluster ring show -unitname vifmgr</code></td>
</tr>
<tr>
<td>SAN management daemon</td>
<td><code>cluster ring show -unitname bcomd</code></td>
</tr>
</tbody>
</table>

**Example**

This example shows the volume location database process:

```
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. 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.

**Example**

```
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 ...
```

5. Return to the admin privilege level:

```
set -privilege admin
```

**Verifying storage health**

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

**Steps**

1. If you are preparing to upgrade, revert, or downgrade, verify disk status:

   **To check for...**
   **Do this...**

   **Broken disks**
   - 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 reconstruction | 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 finish before proceeding.

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates:

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

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

**Example**

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

3. Verify that all volumes are online by displaying any volumes that are not online:

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

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

**Example**

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

**Related information**

*Clustered Data ONTAP 8.3 Logical Storage Management Guide*

*Clustered Data ONTAP 8.3 Physical Storage Management Guide*

**Verifying the system time**

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

**Steps**

1. Verify that the cluster is associated with an NTP server:

<table>
<thead>
<tr>
<th>If you are running...</th>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data ONTAP 8.2.x</td>
<td><code>system services ntp server show</code></td>
</tr>
<tr>
<td>Data ONTAP 8.3.x</td>
<td><code>cluster time-service ntp server show</code></td>
</tr>
</tbody>
</table>

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

```
cluster date show
```

**Example**

```
cluster1::> cluster date show
Node       Date                Timezone
---------- ------------------- -------------------------
node0      4/6/2013 20:54:38   GMT
```
Related information

Clustered Data ONTAP 8.3 System Administration 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.

Verifying that the netgroup file is present on all nodes

If you have loaded netgroups into Storage Virtual Machines (SVMs), before you upgrade or revert, you must verify that the netgroup file is present on each node. A missing netgroup file on a node can cause an upgrade or revert to fail.

About this task

For more information about netgroups and loading them from a URI, see the Clustered Data ONTAP File Access Management Guide for NFS.

Steps

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

2. Display the netgroup status for each SVM:
   ```
   vserver services netgroup status
   ```

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

4. Verify that for each SVM, each node shows the same netgroup file hash value.
   If this is the case, you can skip the next step and proceed with the upgrade or revert. Otherwise, proceed to the next step.

5. On any one node of the cluster, manually load the netgroup file to ensure that they are consistent across all nodes:
   ```
   vserver services netgroup load -vserver vserver_name -source uri
   ```
   This command downloads the netgroup file on all nodes. If a netgroup file already exists on a node, it is overwritten.

Configuring Storage Encryption with IPv4 key management servers

Storage Encryption does not support IPv6 networking in Data ONTAP versions earlier than 8.3. If you have configured the system to use Storage Encryption and configured Storage Encryption with IPv6 IP addresses for key management server communications, you must first configure Storage Encryption with key management servers with IPv4 IP addresses instead; otherwise, the revert operation fails.

Steps

1. Obtain IPv4 SSL certificates for each key management server you want to use with Storage Encryption after reverting from Data ONTAP 8.3.
2. Install the public certificate of the key management server:

```
security certificate install -vserver admin_svm_name -type server-ca -subtype kmip-cert -kmip-server-ip key_management_server_ipaddress
```

3. Add a key management server with an IPv4 address:

```
security key-manager add -address key_management_server_ipv4address
```

4. If you are linking multiple key management servers to the cluster, repeat the previous steps for each public certificate of each key management server.

You can link up to four key management servers.

5. Verify that the key management servers have been added and are available:

```
security key-manager show -status
```

6. Remove all IPv6 key management servers:

```
security key-manager delete -address key_management_server_ipv6address
```

7. Verify that only key management servers with IPv4 addresses are configured:

```
security key-manager show -status
```

**Reverting systems with deduplicated volumes**

Before reverting from the Data ONTAP 8.3 release family, you must ensure that the volumes contain sufficient free space for the revert operation.

**Before you begin**

The volume must have enough space to accommodate the savings that were achieved through the inline detection of blocks of zeros. For information about the space required, contact technical support.

**About this task**

Reverting from a Data ONTAP 8.3 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 `set -privilege advanced` command to log in at the advanced privilege level.
4. Use the `volume efficiency revert-to` command with the `-version` option to downgrade the efficiency metadata of a volume to a specific version of Data ONTAP.

   **Example**
   
   The following command reverts the efficiency metadata on volume VolA to the 8.2 version:
   ```
   volume efficiency revert-to -vserver vs1 -volume VolA -version 8.2
   ```

   **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.

5. Use the `volume efficiency show` command with the `-op-status` option to monitor the progress of the downgrade.

   **Example**
   
   The following command monitors and displays the status of the downgrade:
   ```
   volume efficiency show -vserver vs1 -op-status Downgrading
   ```

6. If the revert does not succeed, use the `volume efficiency show` command with the `-instance` option to see why the revert failed.

   **Example**
   
   The following command displays detailed information about all fields:
   ```
   volume efficiency show -vserver vs1 -volume vol1 -instance
   ```

7. After the revert operation is complete, return to the admin privilege level:

   ```
   set -privilege admin
   ```

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

**Reverting systems with compressed volumes**

Before reverting, you must ensure that the volumes contain sufficient free space for the revert operation.

**Before you begin**

For adaptive compression enabled volumes, you must delete all the Snapshot copies and decompress all of the data in the volumes.

**About this task**

Reverting 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 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 volumes:
   ```
   volume efficiency stop {-op-status !Idle} -all true
   ```
2. Use the `volume efficiency show` command to ensure that there are no active and queued data compression operations on the volumes. If any efficiency operations are active, wait for them to be cleared.

Example
The following command displays the progress of efficiency operations:

```
volume efficiency show -op-status !Idle
```

3. Use the `set -privilege advanced` command to log in at the advanced privilege level.

4. If you are reverting to Data ONTAP 8.3, use the `volume efficiency revert-to` command to downgrade the efficiency metadata of a volume. If there are any Snapshot copies with data that was compressed by adaptive compression, they will be displayed. Delete the Snapshot copies before reverting. If prompted, use the `volume efficiency undo` command to decompress the compressed data.

   **Note:** Adaptive compression will not be supported unless all the nodes in the cluster are running Data ONTAP 8.3.1.

Example
The following command downgrades the efficiency metadata on volumes:

```
volume efficiency revert-to -vserver * -volume * -revert-adaptive-compression true
```

5. If you are reverting to releases earlier than Data ONTAP 8.3, use the `volume efficiency revert-to` command with the `-version` option to downgrade the efficiency metadata of a volume. If there are any Snapshot copies with data that was compressed by adaptive compression, they will be displayed. Delete the Snapshot copies before reverting. If prompted, use the `volume efficiency undo` command to decompress the compressed data.

Example
The following command downgrades the efficiency metadata to the 8.2 version:

```
volume efficiency revert-to -vserver * -volume * -version 8.2
```

6. Use the `volume efficiency prepare-to-downgrade` command to update the efficiency configurations and metadata to be compatible with releases before Data ONTAP 8.3.1.

Example
The following command updates the efficiency configurations and metadata to be compatible with releases before Data ONTAP 8.3.1:

```
volume efficiency prepare-to-downgrade
```

7. Use the `volume efficiency show` command with the `-op-status` option to monitor the progress of the downgrade.

Example
The following command monitors and displays the status of the downgrade:

```
volume efficiency show -vserver * -op-status Downgrading
```

8. If the revert does not succeed, use the `volume efficiency show` command with the `-instance` option for details.
Example

The following command displays detailed information about all fields:

```bash
volume efficiency show -vserver vs1 -volume vol1 -instance
```

9. After the revert operation is completed, 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*.

Reverting systems that have the SP automatic configuration enabled

If you have the SP automatic configuration enabled, you must disable the SP automatic configuration, delete subnets, and manually configure the SP network interface before reverting to the Data ONTAP 8.2 release family.

Steps

1. Disable the SP automatic configuration by using the `system service-processor network auto-configuration disable` command.

   The SP automatic configuration has dependencies on subnets, which are not supported in releases prior to Data ONTAP 8.3 and are deleted prior to the reversion. Therefore, you must first disable the SP automatic configuration.

   The `system service-processor network auto-configuration show` command displays the setup for the SP automatic configuration.

2. Delete subnets by using the `network subnet delete` command.

   If the SP automatic configuration is still enabled when you attempt to delete subnets, Data ONTAP prompts you to disable the SP automatic configuration.

3. Manually configure the SP network interface for each node in the cluster by using the `system service-processor network modify` command.

   After the SP automatic configuration is disabled, a manual configuration of the SP network interface is required. In case a node recovery becomes necessary, the SP is needed for assisting the recovery process. Failure to properly configure the SP network interface might affect the node's ability to recover from a system error.

   When the SP automatic configuration is disabled, the SP port is set up to use IPv4 DHCP and disable IPv6 by default. If the DHCP server in your network is functioning properly, an IPv4 address is assigned to the SP port. You can use the IPv4 DHCP address or manually specify another address to use. The DHCP information for the SP is preserved even after the reversion.

Related information

*Clustered Data ONTAP 8.3 System Administration Guide*

Preparing Snapshot copies before reverting

Before reverting to an earlier Data ONTAP release, you must disable all Snapshot copy policies and delete any Snapshot copies that were created after upgrading to the current release.

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 8.3.x
• All data protection mirror relationships if the cluster was re-created in Data ONTAP 8.3.x

Steps
1. Disable Snapshot copy policies for all data SVMs:
   ```
   volume snapshot policy modify -vserver * -enabled false
   ```

2. Disable Snapshot copy policies for each node's aggregates:
   a. Identify the node's aggregates by using the `run -node nodename aggr status` command.
   b. Disable the Snapshot copy policy for each aggregate:
      ```
      run -node nodename aggr options aggr_name nosnap on
      ```
   c. Repeat this step for each remaining node.

3. Disable Snapshot copy policies for each node's root volume:
   a. Identify the node's root volume by using the `run -node nodename vol status` command.
      You identify the root volume by the word `root` in the `Options` column of the `vol status` command output.
   b. Disable the Snapshot copy policy on the root volume:
      ```
      run -node nodename vol options root_volume_name nosnap on
      ```
   c. Repeat this step for each remaining node.

4. Delete all Snapshot copies that were created after upgrading to the current release:
   a. Set the privilege level to advanced:
      ```
      set -privilege advanced
      ```
   b. Delete the node's newer-version Snapshot copies:
      ```
      volume snapshot prepare-for-revert -node nodename
      ```
      This command deletes the newer-version Snapshot copies on each data volume, root aggregate, and root volume.
      If any Snapshot copies cannot be deleted, the command fails and notifies you of any required actions you must take before the Snapshot copies can be deleted. You must complete the required actions and then rerun the `volume snapshot prepare-for-revert` command before proceeding to the next step.
Example

```
cluster1:~$> volume snapshot prepare-for-revert -node node1
```

Warning: This command will delete all Snapshot copies that have the format used by the current version of Data ONTAP. It will fail if any Snapshot copy polices are enabled, or if any Snapshot copies have an owner. Continue? {y|n}: y

c. Verify that the Snapshot copies have been deleted:

```
volume snapshot show -node nodename
```

If any newer-version Snapshot copies remain, force them to be deleted:

```
volume snapshot delete {--fs-version 8.3 -node nodename -is-constituent true} -ignore-owners -force
```

d. Repeat this step for each remaining node.

e. Return to the admin privilege level:

```
set -privilege admin
```

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.

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, `831_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

*NetApp Downloads: Software*

Installing Data ONTAP software images for a reversion

Before performing a reversion to Data ONTAP 8.2, you must install the target Data ONTAP software image on each node in the cluster.

Before you begin

You must have obtained the Data ONTAP software images.
Steps

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

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download, but not install, the software image</td>
<td><code>system node image get -node * -package location -replace-package true -background true</code>&lt;br&gt;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.</td>
</tr>
<tr>
<td>Install a previously downloaded software image</td>
<td><code>system node image update -node * -package image_name -background true</code>&lt;br&gt;Note the following considerations for this command:&lt;br&gt;• 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.&lt;br&gt;• 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.</td>
</tr>
<tr>
<td>Download and install the software image in the same operation</td>
<td><code>system node image update -node * -package location -replace-package true -background true</code>&lt;br&gt;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.</td>
</tr>
</tbody>
</table>

2. Verify that the software image is downloaded and installed on each node:

`system node image show-update-progress -node *`<br>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 file system 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:
   ```bash
   system image show
   ```
   Example
   This example shows that version 8.2.1 is installed as the alternate image on both nodes:
   ```
   cluster1::> system image show
   Is  Is                 Install
   Node  Image   Default Current Version    Date
   -------- ------- ------- ------- --------   -------------------
   node0  image1  true    true    8.3.1      6/25/2015 12:37:36
   image2  false   false   8.2.1      5/10/2014 13:52:22
   node1  image1  true    true    8.3.1      6/25/2015 12:41:16
   image2  false   false   8.2.1      5/10/2014 13:55:22
   4 entries were displayed.
   ```
2. Disable all of the data LIFs in the cluster:
   ```bash
   network interface modify {-role data} -status-admin down
   ```
3. If the cluster consists of only two nodes, disable cluster HA:
   ```bash
   cluster ha modify -configured false
   ```
4. Disable storage failover for the nodes in the HA pair from either node:
   ```bash
   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.
5. Log in to the node that you want to revert.
   To revert a node, you must be logged in to the cluster through the node’s node management LIF.
6. Set the node’s target Data ONTAP software image to be the default image:
   ```bash
   system image modify -node nodename -image target_image -isdefault true
   ```
7. Verify that the target Data ONTAP software image is set as the default image for the node that you are reverting:
   ```bash
   system image show
   ```
   Example
   This example shows that version 8.2.1 is set as the default image on node0:
Reverting clusters to an earlier Data ONTAP release family | 125

8. Set the privilege level to advanced:
   
   set -privilege advanced

9. If the cluster consists of only two nodes, verify that the node does not hold epsilon:

   a. Check whether the node currently holds epsilon:

      cluster show -node nodename

   **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, 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

10. Verify that the node is ready for reversion:

    system node revert-to -node nodename -check-only true -version 8.2

    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

11. Verify that all of the preconditions have been addressed:

    system node revert-to -node nodename -check-only true -version 8.2

12. Revert the cluster configuration of the node:

    system node revert-to -node nodename -version 8.2

    The `-version` option refers to the target release family. For example, if the software you installed and verified is Data ONTAP 8.2.1, the correct value of the `-version` option is `8.2`.

    The cluster configuration is reverted, and then you are logged out of the clustershell.

13. Log back in to the clustershell, and then switch to the nodeshell:

    run -node nodename
14. Revert the file system configuration of the node:
   ```
   revert_to 8.2
   ```
   This command verifies that the node's file system configuration is ready to be reverted, and then
   reverts it. If any preconditions are identified, you must address them and then reenter the
   revert_to command.

   When the command finishes, the LOADER prompt is displayed.

15. At the LOADER prompt, boot to the target release:
   ```
   boot_ontap
   ```
   You should wait until the login prompt is displayed before proceeding to the next step.

16. Repeat Steps 5 through 15 on the other node in the HA pair.

17. If the cluster consists of only two nodes, reenable cluster HA:
   ```
   cluster ha modify --configured true
   ```

18. Reenable storage failover on both nodes if it was previously disabled:
   ```
   storage failover modify --node nodename --enabled true
   ```

19. Repeat Steps 4 through 18 for each additional HA pair in the cluster.

20. After all nodes have been reverted, reinstall the Data ONTAP 8.2.x image as the alternate image
    on each node:
    ```
    system image update --node * --package location --background true
    ```
    You do not need to boot the image. Reinstalling the Data ONTAP 8.2.x image puts the cluster in a
    state that is necessary for the SVM networking to be verified when you are ready to upgrade back
    to Data ONTAP 8.3.

### 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.

**Steps**

1. **Verifying cluster health** on page 127
   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 that the cluster is in quorum.

2. **Verifying storage health** on page 128
   Before and after you upgrade, revert, or downgrade a cluster, you should verify the status of your
   disks, aggregates, and volumes.

3. **Enabling and reverting LIFs to home ports** on page 129
   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.

4. **Preparing Snapshot copies after reverting** on page 131
   After reverting to an earlier version of Data ONTAP, you must enable Snapshot copy policies to
   start creating Snapshot copies again.

5. **Verifying client access (CIFS and NFS)** on page 131
   For the configured protocols, test access from CIFS and NFS clients to verify that the cluster is
   accessible.

6. **Deleting the system SVM for the Cluster IP space** on page 131
When you revert to Data ONTAP 8.2, IP spaces are removed. However, the system SVM for the Cluster IP space is not removed, and you must manually delete it.

7. **Verifying IPv6 firewall entries** on page 132
   A reversion from Data ONTAP 8.3 might result in missing default IPv6 firewall entries for some services in firewall policies. You need to verify that the required firewall entries have been restored to your system.

8. **Considerations for whether to manually update the SP firmware** on page 133
   If the SP automatic update functionality is enabled (the default), downgrading or reverting to Data ONTAP 8.2.1 or later does not require a manual SP firmware update. The SP firmware is automatically updated to the newest compatible version that is supported by the Data ONTAP version you reverted or downgraded to.

9. **Considerations for dump backups** on page 133
   If you use the dump engine to back up FlexVol volumes, then after reverting to Data ONTAP 8.2, you must perform a baseline backup operation before you can perform any incremental backup operations.

10. **Creating namespace mirror constituents for reverted Infinite Volumes** on page 133
    After reverting a cluster that contains an Infinite Volume to Data ONTAP 8.2.x, you must create one or more namespace mirror constituents. How you create the namespace mirror constituents depends on whether the Infinite Volume uses storage classes and is configured for tape backup.

### Verifying cluster 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 that the cluster is in quorum.

**Steps**

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

2. Set the privilege level to advanced:
   ```bash
   set -privilege advanced
   ```
   Enter `y` to continue.

3. Verify the configuration details for each RDB process.
   You should verify the following configuration details:
   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.
     Note that each ring might have a different quorum master.
To display this RDB process...

<table>
<thead>
<tr>
<th>Management application</th>
<th>cluster ring show -unitname mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume location database</td>
<td>cluster ring show -unitname vldb</td>
</tr>
<tr>
<td>Virtual-Interface manager</td>
<td>cluster ring show -unitname vifmgr</td>
</tr>
<tr>
<td>SAN management daemon</td>
<td>cluster ring show -unitname bcomd</td>
</tr>
</tbody>
</table>

**Example**

This example shows the volume location database process:

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

<table>
<thead>
<tr>
<th>Node</th>
<th>UnitName</th>
<th>Epoch</th>
<th>DB Epoch</th>
<th>DB Trnxs</th>
<th>Master</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>vldb</td>
<td>154</td>
<td>154</td>
<td>14847</td>
<td>node0</td>
<td>master</td>
</tr>
<tr>
<td>node1</td>
<td>vldb</td>
<td>154</td>
<td>154</td>
<td>14847</td>
<td>node0</td>
<td>secondary</td>
</tr>
<tr>
<td>node2</td>
<td>vldb</td>
<td>154</td>
<td>154</td>
<td>14847</td>
<td>node0</td>
<td>secondary</td>
</tr>
<tr>
<td>node3</td>
<td>vldb</td>
<td>154</td>
<td>154</td>
<td>14847</td>
<td>node0</td>
<td>secondary</td>
</tr>
</tbody>
</table>

4 entries were displayed.
```

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.

**Example**

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

<table>
<thead>
<tr>
<th>Time</th>
<th>Node</th>
<th>Severity</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/13/2013 14:03:51 node0</td>
<td>INFORMATIONAL</td>
<td>scsiblade.in.quorum: The scsi-blade ...</td>
<td></td>
</tr>
<tr>
<td>8/13/2013 14:03:51 node1</td>
<td>INFORMATIONAL</td>
<td>scsiblade.in.quorum: The scsi-blade ...</td>
<td></td>
</tr>
</tbody>
</table>
```

5. Return to the admin privilege level:

```
set -privilege admin
```

**Verifying storage health**

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

**Steps**

1. If you are preparing to upgrade, revert, or downgrade, verify disk status:

   **To check for...**

   **Do this...**

   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 reconstruction | 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 finish before proceeding.

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates:

   `storage aggregate show -state !online`

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

   **Example**

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

3. Verify that all volumes are online by displaying any volumes that are not online:

   `volume show -state !online`

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

   **Example**

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

**Related information**

*Clustered Data ONTAP 8.3 Logical Storage Management Guide*
*Clustered Data ONTAP 8.3 Physical 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).
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.
Preparing Snapshot copies after reverting

After reverting to an earlier version of Data ONTAP, you must enable Snapshot copy policies to start creating Snapshot copies again.

About this task

You are reenabling the Snapshot schedules that you disabled before you reverted to an earlier version of Data ONTAP.

Steps

1. Enable Snapshot copy policies for all data SVMs:
   ```bash
   volume snapshot policy modify -vserver * -enabled true
   ```

2. For each node, enable the Snapshot copy policy of the root volume by using the `run -node nodename vol options root_vol_name nosnap off` command.

   Example
   ```bash
   cluster1::> run -node node1 vol options vol0 nosnap off
   ```

3. For each node, enable the Snapshot copy policy of the aggregates by using the `run -node nodename aggr options aggr_name nosnap off` command.

   Example
   ```bash
   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.

Deleting the system SVM for the Cluster IP space

When you revert to Data ONTAP 8.2, IP spaces are removed. However, the system SVM for the Cluster IP space is not removed, and you must manually delete it.

Steps

1. Determine whether the Cluster SVM exists:
   ```bash
   vserver show
   ```

   Example
   ```bash
   cluster1::> vserver show
   Vserver | Type | Admin State | Root Volume | Aggregate | Name Service | Name Mapping
   --------|------|-------------|-------------|-----------|--------------|---------------
   Cluster  | 4    | -           | -           | -         |              |               
   cluster1 | admin| -           | -           | -         |              |               
   node0    | node | -           | -           | -         |              |               
   node1    | node | -           | -           | -         |              |               
   vs0      | data | running     | root        | aggr1     | file         | file          
   ```
2. Delete the Cluster SVM:

```bash
vserver delete -vserver Cluster
```

### Verifying IPv6 firewall entries

A reversion from Data ONTAP 8.3 might result in missing default IPv6 firewall entries for some services in firewall policies. You need to verify that the required firewall entries have been restored to your system.

#### Steps

1. Verify that all firewall policies are correct by comparing them to the default policies:

```bash
system services firewall policy show
```

#### Example

The following example shows the default policies:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Service</th>
<th>Action</th>
<th>IP-List</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster</td>
<td>dns</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>http</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>https</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>ndmp</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>ntp</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>rsh</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>snmp</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>ssh</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>telnet</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>data</td>
<td>dns</td>
<td>allow</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>http</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>https</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>ndmp</td>
<td>allow</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>ntp</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>rsh</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>snmp</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>ssh</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>telnet</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td>intercluster</td>
<td>dns</td>
<td>deny</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>http</td>
<td>deny</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>https</td>
<td>deny</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>ndmp</td>
<td>allow</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>ntp</td>
<td>deny</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>rsh</td>
<td>deny</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>snmp</td>
<td>deny</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>ssh</td>
<td>deny</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td></td>
<td>telnet</td>
<td>deny</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>mgmt</td>
<td>dns</td>
<td>allow</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>http</td>
<td>allow</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>https</td>
<td>allow</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>ndmp</td>
<td>allow</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>ntp</td>
<td>allow</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>rsh</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>snmp</td>
<td>allow</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>ssh</td>
<td>allow</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
<tr>
<td></td>
<td>telnet</td>
<td>deny</td>
<td>0.0.0.0/0, ::/0</td>
</tr>
</tbody>
</table>

2. Manually add any missing default IPv6 firewall entries by creating a new firewall policy:

```bash
system services firewall policy create
```
Considerations for whether to manually update the SP firmware

If the SP automatic update functionality is enabled (the default), downgrading or reverting to Data ONTAP 8.2.1 or later does not require a manual SP firmware update. The SP firmware is automatically updated to the newest compatible version that is supported by the Data ONTAP version you reverted or downgraded to.

If the SP automatic update functionality is disabled (not recommended), after the Data ONTAP revert or downgrade process is complete, you must manually update the SP firmware to a version that is supported for the Data ONTAP version you reverted or downgraded to.

Related information

NetApp BIOS Service Processor Support Matrix
NetApp Downloads: System Firmware and Diagnostics

Considerations for dump backups

If you use the dump engine to back up FlexVol volumes, then after reverting to Data ONTAP 8.2, you must perform a baseline backup operation before you can perform any incremental backup operations.

Related information

Clustered Data ONTAP 8.3 Data Protection Tape Backup and Recovery Guide

Creating namespace mirror constituents for reverted Infinite Volumes

After reverting a cluster that contains an Infinite Volume to Data ONTAP 8.2.x, you must create one or more namespace mirror constituents. How you create the namespace mirror constituents depends on whether the Infinite Volume uses storage classes and is configured for tape backup.

About this task

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. However, if the destination Infinite Volume is configured for incremental tape backup, you must reenable SnapDiff on the destination Infinite Volume to support incremental tape backup.

Choices

• Creating a namespace mirror constituent for a reverted Infinite Volume on page 134
• Reenabling SnapDiff for a reverted Infinite Volume configured for tape backup on page 134
Creating a namespace mirror constituent for a reverted Infinite Volume

After reverting a cluster that contains an Infinite Volume, the namespace mirror constituent is removed. You must create a namespace mirror constituent for the Infinite Volume to provide data protection for the namespace constituent.

Before you begin

- All nodes in the cluster that contain the Infinite Volume must have been reverted to Data ONTAP 8.2.x.
- SnapDiff must be disabled for the Infinite Volume.
- The Infinite Volume must not use storage classes.

Steps

1. 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 require the size of the namespace constituent because the namespace mirror constituent will be the same size as the namespace constituent.

   Example

   In the following example, the namespace constituent is named `repo_vol_ns` and is 10 TB in size.

   ```
   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.
   ```

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.

Reenabling SnapDiff for a reverted Infinite Volume configured for tape backup

After reverting a cluster that contains an Infinite Volume that is configured for tape backup, the namespace mirror constituents are removed. You must reenable SnapDiff to create namespace mirror
constituents for the Infinite Volume to provide data protection for the namespace constituent and to support tape backup.

**Before you begin**

All nodes in the cluster that contain the Infinite Volume must have been reverted to Data ONTAP 8.2.x.

**About this task**

You cannot perform tape backup and restore operations until the namespace mirror constituents are created.

**Step**

1. Reenable SnapDiff for the Infinite Volume by using the `volume modify` command with the `-enable-snapdiff` parameter.

   **Example**

   In the following example, SnapDiff is reenabled for the Infinite Volume named `repo_vol`:

   ```bash
   cluster1:/> volume modify repo_vol -enable-snapdiff true
   [Job 39] Job succeeded: Modified Infinite Volume successfully.
   ```

   Namespace mirror constituents are created on all nodes, except the node with the namespace constituent. One namespace mirror constituent provides data protection for the namespace constituent, and the remaining namespace mirror constituents support incremental tape backup of the Infinite Volume.

**Creating a namespace mirror constituent for a reverted Infinite Volume with storage classes**

After reverting a cluster that contains an Infinite Volume with storage classes, the namespace mirror constituent is removed. You must create a namespace mirror constituent for the Infinite Volume to provide data protection for the namespace constituent by enabling and then disabling SnapDiff.

**Before you begin**

- All nodes in the cluster that contain the Infinite Volume must have been reverted to Data ONTAP 8.2.x.

- You must know the name of the aggregate on each node that you want to use for the namespace mirror constituent, and each aggregate must have 10 TB of free space.

  Each node that contains a data constituent requires a namespace mirror constituent to support SnapDiff, except the node with the namespace constituent.

**About this task**

You create a namespace mirror constituent by first enabling SnapDiff to create multiple namespace mirror constituents, and then disabling SnapDiff to remove all namespace mirror constituents, except one namespace mirror constituent. One namespace mirror constituent is retained to provide data protection for the namespace constituent.

**Steps**

1. Switch to advanced privilege by using the `set -privilege advanced` command.

2. Enable SnapDiff and specify the aggregates on the nodes to use for namespace mirror constituents by using the `volume modify` command with the `-enable-snapdiff` parameter.
Example
In the following example, you have identified an aggregate on each node, aggr9 and aggr13, to contain the namespace mirror constituents. You enable SnapDiff for the Infinite Volume with storage classes named repo_vol and specify two aggregates (one on each node):

```
cluster2::*> volume modify repo_vol -enable-snapdiff true -ns-mirror-aggr-list aggr9 aggr13
```

Namespace mirror constituents are created on all nodes with a data constituent, except the node with the namespace constituent.

3. Disable SnapDiff for the Infinite Volume by using the `volume modify` command with the `-disable-snapdiff` parameter.

Example
In the following example, SnapDiff is disabled for the Infinite Volume named repo_vol:

```
cluster1::*> volume modify repo_vol -enable-snapdiff false
[Job 50] Job succeeded: Modified Infinite Volume successfully.
```

All but one namespace mirror constituent are removed from the Infinite Volume. The remaining namespace mirror constituent provides data protection for the namespace constituent.

Reenabling SnapDiff for a reverted Infinite Volume with storage classes configured for tape backup

After reverting a cluster that contains an Infinite Volume with storage classes that is configured for tape backup, the namespace mirror constituents are removed. You must reenable SnapDiff to create namespace mirror constituents for the Infinite Volume to provide data protection for the namespace constituent and to support tape backup.

Before you begin
- All nodes in the cluster that contain the Infinite Volume with storage classes must have been reverted to Data ONTAP 8.2.x.
- You must know the name of the aggregate on each node that you want to use for the namespace mirror constituent, and each aggregate must have 10 TB of free space.
  Each node that contains a data constituent requires a namespace mirror constituent to support SnapDiff, except the node with the namespace constituent.

About this task
You cannot perform tape backup and restore operations until the namespace mirror constituents are created.

Steps
1. Switch to advanced privilege by using the `set -privilege advanced` command.
2. Reenable SnapDiff and specify the aggregates on the nodes to use for namespace mirror constituents by using the `volume modify` command with the `-enable-snapdiff` parameter.

Example
In the following example, you have identified an aggregate on each node, aggr9 and aggr13, to contain the namespace mirror constituents. You reenable SnapDiff for the Infinite Volume with storage classes named repo_vol and specify two aggregates (one on each new node):
Namespace mirror constituents are created on all nodes, except the node with the namespace constituent. One namespace mirror constituent provides data protection for the namespace constituent, and the remaining namespace mirror constituents support incremental tape backup of the Infinite Volume with storage classes.
Downgrading clusters to an earlier release in the same release family

Transiting 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.

**Cluster downgrade workflow**

You can use the cluster downgrade workflow to plan the downgrade, prepare for the downgrade, perform the downgrade, and complete post-downgrade tasks.
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 downgradable 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.

Steps
1. Reviewing pre-downgrade resources on page 139
2. Downgrade process considerations on page 140
3. Downgrade requirements for MetroCluster configurations on page 140

Reviewing pre-downgrade resources

Before downgrading Data ONTAP, you should review resources to understand issues you must
resolve before downgrading, understand new system behavior in the prior release, and confirm
hardware support.

Steps

   Find the Release Notes for your version of Data ONTAP 8

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

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

   NetApp Hardware Universe

3. Confirm that your cluster and management switches are supported in the target release.
You must verify that the NX-OS (cluster network switches), IOS (management network switches), and reference configuration file (RCF) software versions are compatible with the version of Data ONTAP to which you are downgrading.

NetApp Downloads: Cisco Ethernet Switch

4. If your cluster is configured for SAN, confirm that the SAN configuration is fully supported. All SAN components—including target Data ONTAP software version, host OS and patches, required Host Utilities software, and adapter drivers and firmware—should be supported.

NetApp Interoperability Matrix Tool

Downgrade process considerations

You need to know about downgrade issues and limitations before downgrading clusters to an earlier version of Data ONTAP.

You should be aware of the following issues:

• After you upgrade clusters to Data ONTAP 8.3, you can downgrade to an earlier release in the Data ONTAP 8.3 release family. For example, you can downgrade from Data ONTAP 8.3.y to 8.3.x.

• 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 HA 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 and SQL Server over SMB solutions. These solutions enable the application servers and the contained virtual machines or databases to stay online and to provide continuous availability during the Data ONTAP downgrade. 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. You should complete the upgrade as quickly as possible; do not allow the cluster to remain in a mixed version state longer than necessary.

Related information

Clustered Data ONTAP 8.3 File Access Management Guide for CIFS

Downgrade requirements for MetroCluster configurations

Data ONTAP 8.3 supports MetroCluster configurations. If you have a MetroCluster configuration, you can downgrade Data ONTAP nondisruptively within the 8.3 release family. However, you should be aware of some important requirements.

General requirements

• Both clusters must be running the same version of Data ONTAP. You can verify the Data ONTAP version by using the version command.
• Two-node MetroCluster configurations can only be downgraded to Data ONTAP 8.3.1 or later. This configuration cannot be downgraded to Data ONTAP 8.3.0.

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

• You can downgrade both clusters at the same time, or downgrade one cluster before the other. The downgrade is nondisruptive regardless of which cluster you downgrade first.

• The aggregates in both clusters must not be in resyncing RAID status. During MetroCluster healing, the mirrored aggregates are resynchronized. You can verify whether the MetroCluster configuration is in this state by using the `storage aggregate plex show -in-progress true` command. If any aggregates are in progress, you should not perform a downgrade until the aggregate resynchronization is complete.

• Negotiated switchover operations will fail while the downgrade is in progress. After the downgrade has started, you should not attempt a negotiated switchover until both clusters have been downgraded and all nodes are running the same version of Data ONTAP. If a site failure occurs during the downgrade, you should perform a forced switchover.

• The MetroCluster operation history might not be available after downgrading. If you previously used the `metrocluster check run` command while running Data ONTAP 8.3.1, then after downgrading, the `metrocluster operation show` and `metrocluster operation history show` commands incorrectly display “12” instead of the previous check operation.

Configuration requirements for normal operation

• The source SVM LIFs must be up and located on their home nodes. Data LIFs for the destination SVMs are not required to be up or to be on their home nodes.

• All aggregates at the local site must be online.

• All root and data volumes owned by the local cluster's SVMs must be online.

Configuration requirements for switchover

• All LIFs must be up and located on their home nodes.

• All aggregates must be online, except for the root aggregates at the DR site. Root aggregates at the DR site are offline during certain phases of switchover.

• All volumes must be online.

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.

Steps

1. Verifying that the cluster is ready to be downgraded on page 142
   Before you perform the downgrade, you should verify that your cluster configuration is healthy.

2. Preparing Data ONTAP features for the downgrade on page 148
   If you are downgrading a cluster that you have configured to serve data to clients in your environment, you must ensure that certain configurations are prepared for the downgrade.

3. Obtaining Data ONTAP software images on page 152
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.

**Verifying that the cluster is ready to be downgraded**

Before you perform the downgrade, you should verify that your cluster configuration is healthy.

**Verifying cluster 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 that the cluster is in quorum.

**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.

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

   Enter `y` to continue.

3. Verify the configuration details for each RDB process.

   You should verify the following configuration details:
   
   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.

   Note that each ring might have a different quorum master.

   **To display this RDB process...**
   **Enter this command...**
   
<table>
<thead>
<tr>
<th>Management application</th>
<th>cluster ring show -unitname mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume location database</td>
<td>cluster ring show -unitname vldb</td>
</tr>
<tr>
<td>Virtual-Interface manager</td>
<td>cluster ring show -unitname vifmgr</td>
</tr>
<tr>
<td>SAN management daemon</td>
<td>cluster ring show -unitname bcomd</td>
</tr>
</tbody>
</table>

   **Example**

   This example shows the volume location database process:

   ```
   cluster1::*> cluster ring show -unitname vldb
   Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
   --------- -------- -------- -------- -------- --------- ---------
   node0     vldb     154      154      14847    node0     master
   ```
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.

   Example

   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 ...

5. Return to the admin privilege level:

   set -privilege admin

Verifying storage health

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

Steps

1. If you are preparing to upgrade, revert, or downgrade, verify disk status:

<table>
<thead>
<tr>
<th>To check for...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broken disks</td>
<td>a. Display any broken disks:</td>
</tr>
<tr>
<td></td>
<td>storage disk show -state broken</td>
</tr>
<tr>
<td></td>
<td>b. Remove or replace any broken disks.</td>
</tr>
<tr>
<td>Disks undergoing maintenance or reconstruction</td>
<td>a. Display any disks in maintenance, pending, or reconstructing states:</td>
</tr>
<tr>
<td></td>
<td>storage disk show -state maintenance</td>
</tr>
<tr>
<td></td>
<td>b. Wait for the maintenance or reconstruction operation to finish before proceeding.</td>
</tr>
</tbody>
</table>

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates:

   storage aggregate show -state !online

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

   Example

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

3. Verify that all volumes are online by displaying any volumes that are not online:

   volume show -state !online

   All volumes must be online before and after performing a major upgrade or reversion.
Verifying networking and storage status for MetroCluster configurations

Before and after performing a minor upgrade or downgrade in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

About this task

If you are performing a major upgrade from Data ONTAP 8.2, you do not need to complete this procedure.

Steps

1. Verify the LIF status:

   network interface show

   In normal operation, LIFs for source SVMs must be up and located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs should be up, but they do not need to be located on their home nodes.

Example

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Logical Interface</th>
<th>Admin/Oper Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Port</th>
<th>Is Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1-a1_clust1</td>
<td>up/up</td>
<td>192.0.2.1/24</td>
<td>cluster1-01</td>
<td>e2a</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_clust2</td>
<td>up/up</td>
<td>192.0.2.2/24</td>
<td>cluster1-01</td>
<td>e2b</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_clust1</td>
<td>up/up</td>
<td>192.0.2.3/24</td>
<td>cluster1-02</td>
<td>e2a</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_clust2</td>
<td>up/up</td>
<td>192.0.2.4/24</td>
<td>cluster1-02</td>
<td>e2b</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-01</td>
<td>clus_mgmt</td>
<td>up/up</td>
<td>198.51.100.1/24</td>
<td>cluster1-01</td>
<td>e3a</td>
<td>true</td>
</tr>
<tr>
<td>cluster1-a1_inet4_intercluster1</td>
<td>up/up</td>
<td>198.51.100.2/24</td>
<td>cluster1-01</td>
<td>e3c</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_inet4_intercluster2</td>
<td>up/up</td>
<td>198.51.100.3/24</td>
<td>cluster1-01</td>
<td>e3c</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_mmgmt</td>
<td>up/up</td>
<td>198.51.100.4/24</td>
<td>cluster1-01</td>
<td>e0M</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_inet4_intercluster1</td>
<td>up/up</td>
<td>198.51.100.5/24</td>
<td>cluster1-02</td>
<td>e3c</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_inet4_intercluster2</td>
<td>up/up</td>
<td>198.51.100.6/24</td>
<td>cluster1-02</td>
<td>e3d</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster1-a2_mmgmt</td>
<td>up/up</td>
<td>198.51.100.7/24</td>
<td>cluster1-02</td>
<td>e0M</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>vs1</td>
<td>cluster1-a1_data1</td>
<td>up/up</td>
<td>198.51.100.8/24</td>
<td>cluster1-01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-a1_data2</td>
<td>up/up</td>
<td>198.51.100.9/24</td>
<td>cluster1-01</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. Verify the state of the aggregates:

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

This command displays any aggregates that are not online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

**Example**

This example shows a cluster in normal operation:

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

**Example**

This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are offline:

```
cluster1::> storage aggregate show -state !online

<table>
<thead>
<tr>
<th>Aggregate</th>
<th>Size</th>
<th>Available</th>
<th>Used%</th>
<th>State</th>
<th>#Vols</th>
<th>Nodes</th>
<th>RAID Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggr0_b1</td>
<td>0B</td>
<td>0B</td>
<td>0%</td>
<td>offline</td>
<td>0</td>
<td>cluster2-01</td>
<td>raid_dp, mirror</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>degraded</td>
</tr>
<tr>
<td>aggr0_b2</td>
<td>0B</td>
<td>0B</td>
<td>0%</td>
<td>offline</td>
<td>0</td>
<td>cluster2-02</td>
<td>raid_dp, mirror</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>degraded</td>
</tr>
</tbody>
</table>
```

2 entries were displayed.
3. Verify the state of the volumes:

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

This command displays any volumes that are not online. In normal operation, all root and data volumes owned by the local cluster’s SVMs must be online. However, if the MetroCluster configuration is in switchover, all volumes must be online.

**Example**

This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.

```
cluster1::> volume show -state !online
(volume show)
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----  
vs2-mc    vol1         aggr1_b1     -          RW            -          -     -
vs2-mc    root_vs2     aggr0_b1     -          RW            -          -     -
vs2-mc    vol2         aggr1_b1     -          RW            -          -     -
vs2-mc    vol3         aggr1_b1     -          RW            -          -     -
vs2-mc    vol4         aggr1_b1     -          RW            -          -     -
5 entries were displayed.
```

**Verifying the system time**

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

**Steps**

1. Verify that the cluster is associated with an NTP server:

   **If you are running...**  
   **Enter this command...**  
   - Data ONTAP 8.2.x  
     `system services ntp server show`
   - Data ONTAP 8.3.x  
     `cluster time-service ntp server show`

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

   `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.
```

**Related information**

*Clustered Data ONTAP 8.3 System Administration Guide*

**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                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**
   
   ```
   cluster1::> job show
   Job ID Name                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
   ```
Preparing Data ONTAP features for the downgrade

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

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

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

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

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

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

```
network interface show
```

**Example**

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

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

<table>
<thead>
<tr>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address</th>
<th>Current Node</th>
<th>Current Port</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>data001</td>
<td>up/up</td>
<td>192.0.2.120/24</td>
<td>node0</td>
<td>e0e</td>
<td>true</td>
</tr>
<tr>
<td>data002</td>
<td>up/up</td>
<td>192.0.2.121/24</td>
<td>node0</td>
<td>e0f</td>
<td>true</td>
</tr>
<tr>
<td>data003</td>
<td>up/up</td>
<td>192.0.2.122/24</td>
<td>node0</td>
<td>e2a</td>
<td>true</td>
</tr>
<tr>
<td>data004</td>
<td>up/up</td>
<td>192.0.2.123/24</td>
<td>node0</td>
<td>e2b</td>
<td>true</td>
</tr>
<tr>
<td>data005</td>
<td>up/up</td>
<td>192.0.2.124/24</td>
<td>node1</td>
<td>e0e</td>
<td>true</td>
</tr>
<tr>
<td>data006</td>
<td>up/up</td>
<td>192.0.2.125/24</td>
<td>node1</td>
<td>e0f</td>
<td>true</td>
</tr>
<tr>
<td>data007</td>
<td>up/up</td>
<td>192.0.2.116/24</td>
<td>node1</td>
<td>e2a</td>
<td>true</td>
</tr>
<tr>
<td>data008</td>
<td>up/up</td>
<td>192.0.2.127/24</td>
<td>node1</td>
<td>e2b</td>
<td>true</td>
</tr>
</tbody>
</table>

8 entries were displayed.

**Identifying active CIFS sessions that should be terminated**

Before performing a nondisruptive upgrade or downgrade, 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 or Microsoft SQL Server clients using the SMB 3.0 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
Incoming Data LIF IP Address: 198.51.100.5
Workstation IP address: 203.0.113.20
Authentication Mechanism: NTLMv2
Windows User: CIFSLAB\user1
UNIX User: nobody
Open Shares: 1
Open Files: 2
Open Other: 0
Connected Time: 8m 39s
Idle Time: 7m 45s
Protocol Version: SMB2_1
Continuously Available: No
1 entry was displayed.
```

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:

\texttt{vserver cifs session file show -session-id session\_ID}

\textbf{Example}

\begin{verbatim}
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.
\end{verbatim}

\textbf{Checking for back-end configuration errors}

Before downgrading a storage system that uses array LUNs to an earlier release of Data ONTAP, you need to run the \texttt{storage errors show} command to determine whether there are any back-end configuration errors.

\textbf{Steps}

1. Enter the following command:

\texttt{storage array config show}

2. Based on the result of Step 1, proceed with one of the following options:

\begin{center}
\begin{tabular}{|l|l|}
\hline
\textbf{If...} & \textbf{Then...} \\
\hline
If the \texttt{storage array config show} output does not instruct you to run \texttt{storage errors show} & Proceed with downgrading \\
\hline
If the \texttt{storage array config show} output does instruct you to run \texttt{storage errors show} & Continue to the next step \\
\hline
\end{tabular}
\end{center}

You are instructed to run the \texttt{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:

\texttt{storage errors show}

The \texttt{storage errors show} command provides details, at the array LUN level, as the following example shows:

\textbf{Example}

\begin{verbatim}
DGC_RAID5_1
----------
NAME (Serial #): This Array LUN is only available on one path. Proper configuration requires two paths.
\end{verbatim}
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 the `storage errors show` output and provides information about how to fix them.

Preparing SnapMirror relationships for a nondisruptive upgrade or downgrade

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

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:

   ```shell
   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

   This example quiesces transfers involving the destination volume `vol1` from SVM `vs0.example.com`:

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

3. Verify that all SnapMirror relationships are quiesced:

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

   This command displays any SnapMirror relationships that are not quiesced.

   Example

   This example shows that all SnapMirror relationships are quiesced:

   ```shell
   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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait for the transfers to complete before performing the Data ONTAP upgrade.</td>
<td>Once each transfer completes, the relationship changes to Quiesced status.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Stop the transfers by entering the following command:</td>
<td>This command stops the SnapMirror transfer and restores the destination volume to the last Snapshot copy that was successfully transferred. The relationship is set to Quiesced status.</td>
</tr>
<tr>
<td>snapmirror abort -destination-path</td>
<td></td>
</tr>
<tr>
<td>destination -h</td>
<td></td>
</tr>
<tr>
<td>Note: You must use the -foreground true parameter if you are aborting load-sharing mirror transfers.</td>
<td></td>
</tr>
</tbody>
</table>

Related information

*Clustered Data ONTAP 8.3 Data Protection Guide*

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.

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, 831_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

*NetApp Downloads: Software*

Performing the software downgrade

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
  To nondisruptively downgrade a cluster within the Data ONTAP 8.3 release family, you use the `cluster image update` command to install the target Data ONTAP image on each node, and then downgrade the cluster.

• **Downgrading a Data ONTAP cluster nondisruptively by using OnCommand System Manager** on page 156
  If you are downgrading to Data ONTAP 8.3.1 or later and you prefer a graphic interface, you can use OnCommand System Manager to perform an automated, nondisruptive downgrade.

• **Upgrading or downgrading Data ONTAP nondisruptively for a two-node MetroCluster configuration** on page 157
  You can upgrade or downgrade Data ONTAP nondisruptively for a two-node MetroCluster configuration. This method has several steps: initiating a negotiated switchover, updating the cluster at the “failed” site, initiating switchback, and then repeating the process on the cluster at the other site.

• **Downgrading a Data ONTAP cluster disruptively** on page 160
  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.

**Downgrading a Data ONTAP cluster nondisruptively**

To nondisruptively downgrade a cluster within the Data ONTAP 8.3 release family, you use the `cluster image update` command to install the target Data ONTAP image on each node, and then downgrade the cluster.

**Before you begin**

• You must have satisfied downgrade preparation requirements.

• The cluster must consist of at least two nodes.

• For each HA pair, each node should have one or more ports on the same broadcast domain.
  When a set of nodes is downgraded during a batch downgrade, the LIFs are migrated to the HA partner nodes. If the partners do not have any ports in the same broadcast domain, then the LIF migration fails.

**Steps**

1. If you do not plan to monitor the progress of the downgrade process, use the `event route add-destinations` command to send a notification if the downgrade encounters an error and requires manual intervention.

   *Find more information about configuring the Event Management System.*

**Example**

In this example, if the downgrade pauses due to an error, a notification will be sent to the “test_dest” event destination.
2. Download the target Data ONTAP software package:
   ```
   cluster image package get -url location
   ```
   The software package contains the target Data ONTAP image and firmware, and the set of
downgrade validation rules. This package is downloaded to the cluster package repository on the
root volume of one of the nodes in the cluster.

   **Example**

   ```
   cluster1::> cluster image package get -url http://www.example.com/
   software/8.3/image.tgz
   Software get http://www.example.com/software/8.3/image.tgz started on
   node node0
   Downloading package. This may take up to 10 minutes.
   98% downloaded
   There is no update/install in progress
   Status of most recent operation:
   Run Status: Working
   Exit Status: Success
   Phase: Download
   Exit Message: Processing Package.
   Process package Complete
   ```

3. Verify that the software package is available in the cluster package repository:
   ```
   cluster image package show-repository
   ```

   **Example**

   ```
   cluster1::> cluster image package show-repository
   Package Version  Package Build Time
   ---------------- ------------------
   8.3.0            6/25/2015 10:32:15
   ```

4. Verify that the cluster is ready to be downgraded nondisruptively:
   ```
   cluster image validate -version package_version_number
   ```
   This command checks the cluster components to validate that the downgrade can be completed
nondisruptively, and then provides the status of each check and any required action you must take
before performing the software downgrade.

   You can proceed to the next step after completing all identified required actions.

   **Example**

   ```
   cluster1::> cluster image validate -version 8.3.0
   It can take several minutes to complete validation...
   Pre-update Check       Status      Error-Action
   ---------------------  ---------   -------------------------------------------
   Aggregate status       OK          
   CIFS status            OK          
   Cluster health         OK          
   status
   Disk status            OK          
   High Availability      OK          
   status
   LIF status             OK          
   LIFs on home node      OK          
   MetroCluster           OK          
   ```
configuration status
SnapMirror status       OK
Volume status           OK
mgmt epoch status       OK
mgmt RDB ring status    OK
vifmgr epoch status     OK
vifmgr RDB ring         OK
status
vldb epoch status       OK
vldb RDB ring status    OK
Overall Status          OK
17 entries were displayed.

5. Optional: If desired, generate a software downgrade estimate:

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

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

6. Perform the software downgrade:

   `cluster image update -version package_version_number`

   This command validates that each cluster component is ready to be downgraded, installs the target Data ONTAP image on each node in the cluster, and then performs a nondisruptive downgrade in the background. If an issue is encountered, the update pauses and prompts you to take corrective action. You can use the `cluster image show-update-progress` command to view details about the issue. After correcting the issue, you can resume the update by using the `cluster image resume-update` command.

   If the cluster consists of 2 through 6 nodes, a rolling downgrade is performed.

   If the cluster consists of 8 or more nodes, a batch downgrade is performed by default. If desired, you can use the `--force-rolling` parameter to specify a rolling downgrade instead.

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

Example

```
cluster1::> cluster image update -version 8.3.0
Starting validation for this update. Please wait..
It can take several minutes to complete validation...
Non-Disruptive Check       Status       Error-Action
------------------------------- --------- ---------------
Aggregate status            OK
CIFS status                 OK
Cluster health              OK
status
Disk status                 OK
High Availability           OK
status
LIF status                  OK
LIFs on home node           OK
MetroCluster                OK
configuration status
SnapMirror status           OK
Volume status               OK
mgmt epoch status           OK
mgmt RDB ring status        OK
vifmgr epoch status         OK
vifmgr RDB ring             OK
status
vldb epoch status           OK
vldb RDB ring status        OK
Overall Status              OK
17 entries were displayed.
```
Would you like to proceed with update? {y|n}: y
Starting update...

7. Optional: If necessary, manage the downgrade process:

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Enter this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor the status and estimated duration of the downgrade</td>
<td><code>cluster image show-update-progress</code></td>
</tr>
<tr>
<td>View the log of each transaction that has executed during the downgrade</td>
<td><code>cluster image show-update-log</code></td>
</tr>
<tr>
<td>Pause the downgrade</td>
<td><code>cluster image pause-update</code></td>
</tr>
<tr>
<td>Resume a paused downgrade</td>
<td><code>cluster image resume-update</code></td>
</tr>
<tr>
<td>Cancel the downgrade</td>
<td><code>cluster image cancel-update</code></td>
</tr>
</tbody>
</table>

8. Display the cluster update history to verify that the downgrade was completed successfully for each node:

`cluster image show-update-history`

Example

The Data ONTAP version numbers in the following example are provided for example purposes only:

```
cluster1::> cluster image show-update-history
Status  Package     Start Completion Component ID Previous  Updated
-------- ---------  ----------  ------------  ---------  --------
successful 8.3.x 11/18/2014 11/18/2014  node0        8.3.y     8.3.x
15:20:51    15:44:13
successful 8.3.x 11/18/2014 11/18/2014  node1        8.3.y     8.3.x
15:20:51    16:03:20
2 entries were displayed.
```

Downgrading a Data ONTAP cluster nondisruptively by using OnCommand System Manager

If you are downgrading to Data ONTAP 8.3.1 or later and you prefer a graphic interface, you can use OnCommand System Manager to perform an automated, nondisruptive downgrade.

Before you begin

You must have satisfied downgrade preparation requirements.

About this task

If you are downgrading to a Data ONTAP release prior to 8.3.1, you cannot use OnCommand System Manager to downgrade the cluster. You should perform a downgrade using the CLI.

Steps

1. Log in to OnCommand System Manager by using your cluster administrator credential.
   You can access OnCommand System Manager by pointing your web browser to the IP address of the cluster management LIF.

2. Expand the Cluster hierarchy in the left navigation pane.
3. In the navigation pane, click **Cluster Update**.

4. Follow the steps in the **Cluster Update** wizard to perform the downgrade.

   The Cluster Update wizard installs the target Data ONTAP image on each node, validates the cluster components to ensure that the cluster can be downgraded nondisruptively, and then, based on the number of nodes in the cluster, executes either a rolling or batch downgrade in the background.

**After you finish**

You should complete post-downgrade tasks.

**Upgrading or downgrading Data ONTAP nondisruptively for a two-node MetroCluster configuration**

You can upgrade or downgrade Data ONTAP nondisruptively for a two-node MetroCluster configuration. This method has several steps: initiating a negotiated switchover, updating the cluster at the “failed” site, initiating switchback, and then repeating the process on the cluster at the other site.

**Before you begin**

You must have satisfied upgrade or downgrade preparation requirements.

**About this task**

Two-node MetroCluster configurations do not have local HA pairs. Therefore, this procedure describes how to upgrade Data ONTAP nondisruptively by using the negotiated switchover and switchback operations. If you have a four-node MetroCluster configuration, which does have local HA pairs, do not use this procedure. Instead, you should use either the rolling upgrade method or the automated upgrade method to upgrade Data ONTAP nondisruptively.

**Steps**

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

   ```bash
   system node image update -package package_location
   ```

   **Example**

   ```bash
   cluster_B::> system node image update -package http://www.example.com/NewImage.tgz
   ```

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

   ```bash
   system node image show
   ```

   **Example**

   ```bash
   cluster_B::> system node image show
   Node Is Is Is Install Date
   -------- ------ ------ -------------------------------
   node_B_1 image1  false  false  8.3.x  6/18/2015 09:47:32
   image2  true  true  8.3.y  6/25/2015 18:45:56
   2 entries were displayed.
   ```

3. On the cluster that is not being upgraded, initiate a negotiated switchover:

   ```bash
   metrocluster switchover
   ```
The operation can take several minutes. You can use the `metrocluster operation show` command to verify that the switchover is completed properly.

**Example**

In this example, a negotiated switchover is performed on the remote cluster ("cluster_A"). This causes the local cluster ("cluster_B") to halt so that you can upgrade it.

```
cluster_A::> metrocluster switchover
```

Warning: negotiated switchover is about to start. It will stop all the data Vservers on cluster "cluster_B" and automatically re-start them on cluster "cluster_A". It will finally gracefully shutdown cluster "cluster_B".

Do you want to continue? {y|n}: y

4. Resynchronize the data aggregates on the “surviving” cluster:

```
metrocluster heal -phase aggregates
```

**Example**

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

5. Verify that the healing operation was completed successfully:

```
metrocluster operation show
```

**Example**

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
End Time: 6/25/2015 18:45:56
Errors: -
```

6. Resynchronize the root aggregates on the “surviving” cluster:

```
metrocluster heal -phase root-aggregates
```

**Example**

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

7. Verify that the healing operation was completed successfully:

```
metrocluster operation show
```

**Example**

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: 6/25/2015 18:47:03
Errors: -
```

8. On the upgraded cluster, boot the node from the LOADER prompt:

```
boot_ontap
```
9. Wait for the boot process to finish, and then perform a switchback from the “surviving” cluster:
   `metrocluster switchback`

10. Verify that the switchback was completed successfully:
    `metrocluster operation show`

    **Example**

    ```
    cluster_A::> metrocluster operation show
    Operation: switchback
    State: successful
    Errors: -
    ```

11. Repeat Steps 9 on page 157 through 10 on page 159 on the other cluster.

12. Verify that the MetroCluster configuration is healthy:
    a. Check the configuration:
       `metrocluster check run`

       **Example**

       ```
       cluster_A::> metrocluster check run
       Last Checked On: 6/10/2015 17:10:33
       Component         Result
       ------------------ ---------
       nodes             ok
       lifs              ok
       config-replication ok
       aggregates        ok
       4 entries were displayed.
       ```

       Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.
       To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

       b. Display more detailed results from the `metrocluster check run` command:
          `metrocluster check aggregate show`
          `metrocluster check config-replication show`
          `metrocluster check lif show`
          `metrocluster check node show`

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

    d. Simulate the switchover operation:
       `metrocluster switchover -simulate`

    e. Review the results of the switchover simulation:
       `metrocluster operation show`
f. Return to the admin privilege level:
   ```bash
   set -privilege admin
   ```

g. Repeat Steps 12.a through 12.f on the other cluster.

**After you finish**

You should perform any post-upgrade or post-downgrade tasks.

**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.

**Before you begin**

- You must have satisfied downgrade preparation requirements.
- If you are operating in a SAN environment, all SAN clients must be shut down or suspended until the downgrade is complete.
  If SAN clients are not shut down or suspended prior to a disruptive downgrade, the client file systems and applications will suffer errors that might require manual recovery after the downgrade is completed.
- If you want to downgradethe nodes in batches, you must have determined the downgrade sequence.
  You can only upgrade nodes in batches if the cluster consists of at least eight nodes.

**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 8.3 software is installed:
   ```bash
   system node image show
   ```

**Example**

This example shows that version 8.3.x is installed as the alternate image on both nodes:

```
Example

cluster1::> system node image show
   Node          Image  Is  Is  Current Version  Install Date
   --------      ------- ------ --------           ------------
   node0
   image1       true   true   8.3.y      11/27/2014 13:52:22
   image2       false  false   8.3.x      8/27/2014 12:37:36
   node1
   image1       true   true   8.3.y      11/27/2014 13:55:22
   image2       false  false   8.3.x      8/27/2014 12:41:16
4 entries were displayed.
```
2. Change the current default boot image to 8.3.x:

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

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 and then reenter the `system image modify` command.

**Example**

This example shows that the default boot image will be changed to 8.3.x:

```
cluster1::> system image modify {-node * -iscurrent false} -isdefault true
2 entries were modified.
```

3. Redisplay the default boot image:

```
system node image show
```

**Example**

This example shows version 8.3.x as the default image on both nodes:

```
cluster1::> system node image show

<table>
<thead>
<tr>
<th>Node</th>
<th>Image</th>
<th>Default</th>
<th>Current Version</th>
<th>Install Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>image1 false true 8.3.y 11/27/2014 13:52:22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>node1</td>
<td>image2 true false 8.3.x 8/27/2014 12:37:36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>node0</td>
<td>image1 false true 8.3.y 11/27/2014 13:55:22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>node1</td>
<td>image2 true false 8.3.x 8/27/2014 12:41:16</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

4 entries were displayed.

4. Perform one of the following actions:

<table>
<thead>
<tr>
<th>If the cluster consists of...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>One node</td>
<td>Continue to the next step.</td>
</tr>
</tbody>
</table>
| Two nodes                     | a. Disable cluster high availability:  
```
cluster ha modify -configured false
```

b. Disable storage failover for the HA pair:
```
storage failover modify -node * -enabled false
```

| More than two nodes           | Disable storage failover for each HA pair in the cluster:  
```
storage failover modify -node * -enabled false
```

5. Reboot one or more nodes.

<table>
<thead>
<tr>
<th>If...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| The cluster consists of fewer than eight nodes | Reboot a node in the cluster:  
```
system node reboot -node nodename
```

**Attention:** Do not reboot more than one node at a time.

| The cluster consists of eight or more nodes | Reboot each node in the set:  
```
system node reboot -node nodename
```

You must follow the batch upgrade sequence guidelines to determine which nodes can be rebooted concurrently.
The node boots the new Data ONTAP image. The Data ONTAP login prompt appears, indicating that the reboot process is complete.

6. When the node or set of nodes have rebooted with the new Data ONTAP image, confirm that the new Data ONTAP 8.3.x software is running:

```
system node image show
```

Example

This example shows version 8.3.x as the current version on node0:

```
cluster1::> system node image show

+----------+-------+-------+----------+---------------+
<table>
<thead>
<tr>
<th>Node</th>
<th>Image</th>
<th>Default</th>
<th>Current</th>
<th>Install Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>node0</td>
<td>image1</td>
<td>false</td>
<td>false</td>
<td>8.3.y</td>
</tr>
<tr>
<td>node0</td>
<td>image2</td>
<td>true</td>
<td>true</td>
<td>8.3.x</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8/27/2014 12:37:36</td>
</tr>
<tr>
<td>node1</td>
<td>image1</td>
<td>false</td>
<td>true</td>
<td>8.3.y</td>
</tr>
<tr>
<td>node1</td>
<td>image2</td>
<td>true</td>
<td>false</td>
<td>8.3.x</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8/27/2014 12:41:16</td>
</tr>
</tbody>
</table>

4 entries were displayed.
```

7. Repeat Steps 5 through 6 for each additional node.

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

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

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

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

Related tasks

- **Planning the upgrade sequence for a batch upgrade** on page 29
  If you intend to perform a nondisruptive batch upgrade, you should plan the upgrade sequence before you upgrade Data ONTAP. By following the required sequence, you can ensure that the cluster remains up and continues serving data while you perform the NDU.

**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.

**Steps**

1. **Verifying cluster health** on page 163
   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 that the cluster is in quorum.

2. **Verifying storage health** on page 164
   Before and after you upgrade, revert, or downgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

3. **Verifying networking and storage status for MetroCluster configurations** on page 165
   Before and after performing a minor upgrade or downgrade in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

4. **Enabling and reverting LIFs to home ports** on page 167
   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.
5. **Verifying client access (CIFS and NFS) on page 168**
   For the configured protocols, test access from CIFS and NFS clients to verify that the cluster is accessible.

6. **Resuming SnapMirror operations on page 168**
   After completing a nondisruptive upgrade or downgrade, you must resume any SnapMirror relationships that were suspended.

7. **Considerations for whether to manually update the SP firmware on page 169**
   If the SP automatic update functionality is enabled (the default), downgrading or reverting to Data ONTAP 8.2.1 or later does not require a manual SP firmware update. The SP firmware is automatically updated to the newest compatible version that is supported by the Data ONTAP version you reverted or downgraded to.

**Verifying cluster 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 that the cluster is in quorum.

**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.

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

   Enter `y` to continue.

3. Verify the configuration details for each RDB process.
   
   You should verify the following configuration details:

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

   Note that each ring might have a different quorum master.

   **To display this RDB process...** | **Enter this command...**
   --- | ---
   Management application | `cluster ring show -unitname mgmt`
   Volume location database | `cluster ring show -unitname 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:
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.

**Example**

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

<table>
<thead>
<tr>
<th>Time</th>
<th>Node</th>
<th>Severity</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/13/2013 14:03:51</td>
<td>node0</td>
<td>INFORMATIONAL</td>
<td>scsiblade.in.quorum: The scsi-blade ...</td>
</tr>
<tr>
<td>8/13/2013 14:03:51</td>
<td>node1</td>
<td>INFORMATIONAL</td>
<td>scsiblade.in.quorum: The scsi-blade ...</td>
</tr>
</tbody>
</table>

5. Return to the admin privilege level:

```
set -privilege admin
```

**Verifying storage health**

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

**Steps**

1. If you are preparing to upgrade, revert, or downgrade, verify disk status:

   **To check for...**
   **Do this...**

   **Broken disks**
   a. Display any broken disks:
      ```
      storage disk show -state broken
      ```
   b. Remove or replace any broken disks.

   **Disks undergoing maintenance or reconstruction**
   a. Display any disks in maintenance, pending, or reconstructing states:
      ```
      storage disk show -state maintenance|pending|reconstructing
      ```
   b. Wait for the maintenance or reconstruction operation to finish before proceeding.

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates:

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

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

   **Example**

   ```
   cluster1::> storage aggregate show -state !online
   There are no entries matching your query.
   ```
3. Verify that all volumes are online by displaying any volumes that are *not* online:

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

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

**Example**

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

**Related information**

*Clustered Data ONTAP 8.3 Logical Storage Management Guide*
*Clustered Data ONTAP 8.3 Physical Storage Management Guide*

### Verifying networking and storage status for MetroCluster configurations

Before and after performing a minor upgrade or downgrade in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

**About this task**

If you are performing a major upgrade from Data ONTAP 8.2, you do not need to complete this procedure.

**Steps**

1. Verify the LIF status:

```bash
network interface show
```

In normal operation, LIFs for source SVMs must be up and located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs should be up, but they do not need to be located on their home nodes.

**Example**

```
cluster1::> network interface show
Logical Interface Admin/Oper Network Address/Mask Current Port Is Home
-------- ----------- ------------------ ------------- ------ ----
clus_mgmt  up/up    198.51.100.1/24 cluster1-01 e3a   true
cluster1-a1_clus1 up/up    192.0.2.1/24     cluster1-01 e2a   true
cluster1-a2_clus1 up/up    192.0.2.3/24     cluster1-02 e2a   true
cluster1-a1_clus2 up/up    192.0.2.2/24     cluster1-01 e2b   true
cluster1-a2_clus2 up/up    192.0.2.4/24     cluster1-02 e2b   true
cluster1-01
clus_mgmt  up/up    198.51.100.1/24 cluster1-01 e3a   true
cluster1-a1_inet4_intercluster1 up/up 198.51.100.2/24 cluster1-01 e3c   true
cluster1-a1_inet4_intercluster2 up/up 198.51.100.3/24 cluster1-01
cluster1-a1_mgmt1 up/up    198.51.100.4/24 cluster1-01 e0M   true
cluster1-a2_inet4_intercluster1 up/up 198.51.100.5/24 cluster1-02 e3c   true
cluster1-a2_inet4_intercluster2 up/up 198.51.100.6/24 cluster1-02 e3d   true
cluster1-a2_mgmt1
```
2. Verify the state of the aggregates:

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

This command displays any aggregates that are *not* online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

**Example**

This example shows a cluster in normal operation:

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

**Example**

This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are offline:

```
cluster1::> storage aggregate show -state !online

```

<table>
<thead>
<tr>
<th>Aggregate</th>
<th>Size</th>
<th>Available</th>
<th>Used%</th>
<th>State</th>
<th>#Vols</th>
<th>Nodes</th>
<th>RAID Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggr0_b1</td>
<td>0B</td>
<td>0B</td>
<td>0%</td>
<td>offline</td>
<td>0</td>
<td>cluster2-01</td>
<td>raid_dp, mirror degraded</td>
</tr>
</tbody>
</table>
3. Verify the state of the volumes:

   `volume show -state !online`

This command displays any volumes that are not online. In normal operation, all root and data volumes owned by the local cluster's SVMs must be online. However, if the MetroCluster configuration is in switchover, all volumes must be online.

**Example**

This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.

```
cluster1::> volume show -state !online
(volume show)
Vserver Volume Aggregate State Type Size Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- ----- 
vs2-mc vol1 aggr1_b1 - RW - -
vs2-mc root_vs2 aggr0_b1 - RW - -
vs2-mc vol2 aggr1_b1 - RW - -
vs2-mc vol3 aggr1_b1 - RW - -
vs2-mc vol4 aggr1_b1 - RW - -
5 entries were displayed.
```

**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 Network Address/Mask Current Node Current Port Current 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.

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Interface</th>
<th>Status</th>
<th>Network</th>
<th>Current Node</th>
<th>Current Port</th>
<th>Current Is Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs0</td>
<td>data001</td>
<td>up/up</td>
<td>192.0.2.120/24</td>
<td>node0</td>
<td>e0e</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>data002</td>
<td>up/up</td>
<td>192.0.2.121/24</td>
<td>node0</td>
<td>e0f</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>data003</td>
<td>up/up</td>
<td>192.0.2.122/24</td>
<td>node0</td>
<td>e2a</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>data004</td>
<td>up/up</td>
<td>192.0.2.123/24</td>
<td>node0</td>
<td>e2b</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>data005</td>
<td>up/up</td>
<td>192.0.2.124/24</td>
<td>node1</td>
<td>e0e</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>data006</td>
<td>up/up</td>
<td>192.0.2.125/24</td>
<td>node1</td>
<td>e0f</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>data007</td>
<td>up/up</td>
<td>192.0.2.126/24</td>
<td>node1</td>
<td>e2a</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>data008</td>
<td>up/up</td>
<td>192.0.2.127/24</td>
<td>node1</td>
<td>e2b</td>
<td>true</td>
</tr>
</tbody>
</table>

   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 *

This command resumes the transfers for all quiesced SnapMirror relationships.

2. Verify that the SnapMirror operations have resumed:

snapmirror show

Example

<table>
<thead>
<tr>
<th>Source Path</th>
<th>Type</th>
<th>Destination Path</th>
<th>Mirror Status</th>
<th>Relationship Status</th>
<th>Total</th>
<th>Progress</th>
<th>Healthy</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1-vs1:dp_src1</td>
<td>DP</td>
<td>cluster1-vs2:dp_dst1</td>
<td>Snapmirrored</td>
<td>Idle</td>
<td>-</td>
<td>true</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1-vs1:xdp_src1</td>
<td>XDP</td>
<td>cluster1-vs2:xdp_dst1</td>
<td>Snapmirrored</td>
<td>Idle</td>
<td>-</td>
<td>true</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1://cluster1-vs1/ls_src1</td>
<td>LS</td>
<td>cluster1://cluster1-vs1/ls_mr1</td>
<td>Snapmirrored</td>
<td>Idle</td>
<td>-</td>
<td>true</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster1://cluster1-vs1/ls_mr2</td>
<td>Snapmirrored</td>
<td>Idle</td>
<td>true</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 entries were displayed.

For each SnapMirror relationship, verify that the Relationship Status is "Idle". If the status is "Transferring", wait for the SnapMirror transfer to complete, and then reenter the command to verify that the status has changed to "Idle".

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 whether to manually update the SP firmware

If the SP automatic update functionality is enabled (the default), downgrading or reverting to Data ONTAP 8.2.1 or later does not require a manual SP firmware update. The SP firmware is automatically updated to the newest compatible version that is supported by the Data ONTAP version you reverted or downgraded to.

If the SP automatic update functionality is disabled (not recommended), after the Data ONTAP revert or downgrade process is complete, you must manually update the SP firmware to a version that is supported for the Data ONTAP version you reverted or downgraded to.

Related information

NetApp BIOS Service Processor Support Matrix
NetApp Downloads: System Firmware and Diagnostics
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.

Considerations for services and protocols during upgrades

In general, services based on stateless protocols—such as NFSv3, 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 the recommended guidelines listed in the Interoperability Matrix.

Related information

*NetApp Interoperability Matrix Tool*

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 and SQL Server over SMB support nondisruptive operations (NDOs). If you configured a Hyper-V or SQL Server over SMB solution, the application servers and the contained virtual machines or databases remain online and provide continuous availability during the Data ONTAP upgrade.
  For all other CIFS configurations, client sessions are terminated. You should direct users to end their sessions before you upgrade.

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

- **NDMP**
  State is lost and the client user must retry the operation.

- **Backups and restores**
  State is lost and the client user must retry the operation.
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.

How firmware is updated during the Data ONTAP upgrade

Because upgrading Data ONTAP includes upgrading your firmware, you do not need to update firmware manually. When you perform a Data ONTAP upgrade, the firmware for your cluster included with the Data ONTAP upgrade package is copied to each node's boot device, and the new firmware is installed automatically.

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

- System and diagnostics:
  - BIOS
  - Flash Cache
  - Service Processor (SP)
- Disk
- Disk shelf

If desired, you can also update firmware manually in between Data ONTAP upgrades.

Related information

- NetApp Downloads: System Firmware and Diagnostics
- NetApp Downloads: Disk Drive and Firmware
- NetApp Downloads: Disk Shelf Firmware

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.

**Related information**

*Clustered Data ONTAP 8.3 Physical Storage Management Guide*
Upgrading Data ONTAP Edge storage systems

You must perform a few additional preparatory steps to upgrade Data ONTAP Edge storage systems to the latest version of Data ONTAP software.

Data ONTAP Edge systems 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 Edge storage 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.
   - Be prepared to 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.

4. Copy the image to your storage system or to an HTTP or FTP server on your network.

5. Install the Data ONTAP software image on your storage system.
   Extract the system files from the software image you copied to your system.

6. 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.

7. Verify that the version of dvadmin (the Data ONTAP-v administration tool) is compatible with your upgrade target release. dvadmin 1.3 is required when using Data ONTAP 8.3 software. 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.

8. Verify that your systems are operating as expected after the upgrade. Before returning storage systems to production, you should check the status of configured functionalities and reenable 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 Edge 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 Edge system upgrade**

Before installing the latest Data ONTAP release on your storage system, you need to verify some information and complete a few 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 by entering the following dvadmin command:
   ```bash
   vm config backup vm_name backup_name
   ```
   - The backup includes the virtual machine configuration and all information on the Data ONTAP-v system disks.
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:
   ```bash
   storage disk show
   ```
4. Confirm that there are no failed disks:
   ```bash
   storage disk show -state broken
   ```
5. Verify that all aggregates are online:
   ```bash
   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 at the advanced privilege level 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 Edge systems**

You must have access to software images to upgrade the storage system to the latest release of Data ONTAP. Software images are available on the NetApp Support Site.

You can copy software images to an HTTP or FTP server on your network; Data ONTAP Edge storage systems can then access the images by using the `system node image` command.

Software images are specific to storage system models. You must obtain the correct image for your system.

**Related information**

*Download Software: support.netapp.com/NOW/cgi-bin/software*

**Copying the software image to an HTTP or FTP server**

If you have an HTTP or FTP server that is accessible to your storage system, you can copy Data ONTAP software images to that server. This task prepares the HTTP or FTP 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, `830_v_image.tgz`) from the NetApp Support Site to the directory on the HTTP or FTP server from which the file will be served.

**Copying the software image from the HTTP or FTP 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, 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 `830_v_image.tgz` to the storage system:

```bash
system node image get -package http://www.example.com/downloads/x86-64/830_v_image.tgz
```

You see a message similar to the following:

```
software: copying to /etc/software/830_v_image.tgz
software: 100% file read from location.
software: /etc/software/830_v_image.tgz has been copied.
```

Software image installation on Data ONTAP Edge 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/830_v_image.tgz`.
- The URL that provides the location of the package to be downloaded.
  Standard URL schemes, including HTTP and FTP, are accepted.

The `system node image update` command enables 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 or FTP server or from a software image you copied to the storage system.

Step

1. From the storage system prompt, install the software image:

   ```bash
   system node image update -package {url|file_name} options
   ```

   - `url` is the URL of the HTTP or FTP 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:
     1. The `-replace-package` option overwrites the existing image in the `/etc/software` directory when you install software from an HTTP server.
     2. 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

The following command updates the software image on the current node from a software package located at `ftp://ftp.example.com/downloads/830_v_image.tgz`:

Verifying Data ONTAP Edge system status after an upgrade

You should verify that upgraded systems are functioning as expected before returning them to production. This entails verifying the status of configured functionality and reenabling any functionality that was suspended before the upgrade.

About this task

You should perform these tasks on each system that was upgraded.

Steps

1. Verify that the intended target release is installed and running:
   ```
   version
   ```

2. Confirm that all paths to disks are visible to the system:
   ```
   storage disk show
   ```

3. Confirm that there are no failed disks:
   ```
   storage disk show -broken
   ```

4. Verify that all aggregates are online:
   ```
   storage aggr show
   ```

5. Confirm that network interfaces are online:
   ```
   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 © 1994–2016 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, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, 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. A current list of NetApp trademarks is available on the web at http://www.netapp.com/us/legal/netapptmlist.aspx.
How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

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.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

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

32-bit aggregates
  expanding to the 64-bit format 60
32-bit capability
  disabling before upgrade 59
32-bit data
  considerations regarding, for upgrades 25
  finding and removing, after expanding to 64-bit 61
64-bit
  finding and removing 32-bit data after expanding to 61
64-bit aggregates
  expanding 32-bit aggregates to 60

A
ACLs
  setting desired NT display level for NFS clients 107
aggregates
  deduplicated, verifying space for 38
  disabling 32-bit capability before performing cluster upgrades 59
  expanding to the 64-bit format 60
  finding and removing 32-bit data after expanding to 64-bit 61
  verifying health of 34, 97, 114, 128, 143, 164
automated downgrades
  performing using OnCommand System Manager 156
automated upgrades
  definition of nondisruptive cluster 17
  performing nondisruptive cluster 85
  performing using OnCommand System Manager 88
automatic configuration
  SP, reverting systems that have it enabled 120

B
back-end configurations
  finding errors before downgrading 150
background disks
  understanding firmware updates for 172
back-out plans
  for Data ONTAP Edge upgrades 174
backups
  post-reversion considerations for dump 133
batch upgrades
  definition of nondisruptive cluster 17
  disabling automatic LIF rebalancing before 46
  process for cluster 73
  reenabling automatic LIF rebalancing after 103
  upgrading the first set of nodes in a batch of HA pairs 74
  upgrading the set of partner nodes in a batch of HA pairs 79
  verifying cluster version 95

C
checklists
for upgrade 7
CIFS
  considerations for avoiding interruptions during upgrades 171
  identifying active sessions before downgrading 53, 149
  identifying active sessions before upgrading 53, 149
  verifying client access for 131, 168
cluster downgrades
  issues to know before performing 140
  performing nondisruptive, using OnCommand System Manager for 156
cluster HA
  verifying status of 32
cluster health
  verifying 33, 96, 113, 127, 142, 163
Cluster IP space
  deleting the system SVM for 131
cluster reversions
  overview of 109
cluster upgrades
  firmware components that are updated automatically during Data ONTAP 172
  performing nondisruptive, using automated method 85
  performing nondisruptive, using OnCommand System Manager for 88
  process for nondisruptive batch method for 73
  requirements for 21
cluster version
  verifying after upgrade 95
clusters
  downgrade process for 152
  downgrade workflow for 138
  downgrades
    completing post-downgrade tasks 162
    to earlier release in same release family, overview of 138
  downgrading disruptively 160
  downgrading nondisruptively 153
  ensuring that no jobs are running before upgrading or downgrading 42, 146
  how epsilon affects the upgrade sequence of four-node 22
  introduction to performing software upgrades 62
  introduction to planning for reversions of 110
  introduction to preparing features for downgrade 148
  introduction to preparing features for reversion 116
  introduction to preparing to revert 113
  introduction to reversion requirements for 111
  introduction to upgrade requirements for 21
  introduction to verifying health of, before a downgrade 142
  introduction to verifying health of, before a reversion 113
  overview of reversion to an earlier release family 109
  preparation for upgrades 31
  preparing features before upgrade 43
reversion issues and limitations to consider before reverting 111
revert workflow for 109
reverting 124
upgrade workflow for 6
upgrades, planning 20
upgrades, process overview 6
upgrading disruptively 92
upgrading nondisruptively in SnapMirror environments 54, 151
verifying CIFS and NFS client access for 131, 168
verifying health 33, 96, 113, 127, 142, 163
verifying health of before an upgrade 31
verifying that system time is synchronized 41, 115, 146
verifying upgrade limits for 28
command
software update, for installing software images on Data ONTAP Edge systems 177
comments
how to send feedback about documentation 181
compressed volumes
reverting systems with 118
Config Advisor
checking for common configuration errors 32
checking for common configuration errors with 31
downloading and running 31, 32
configuration requirements
for cluster upgrades 21
configurations
checking for errors in back-end 150
SAN, verifying after upgrade 103
SAN, verifying prior to upgrade 41
configurations, MetroCluster two-node
downgrading Data ONTAP for 89, 157
upgrading Data ONTAP for 89, 157
configured clusters
introduction to preparing features for downgrading 148
introduction to preparing features for reverting 116
considerations
cluster downgrade 140

Data ONTAP-v software images
copying from the HTTP or FTP server to the storage system 176
installing from HTTP or FTP servers 177
Data ONTAP-v system files
copying the software image to HTTP or FTP servers 176
data protection mirror relationships
considerations when upgrading Infinite Volumes 26
deduplicated volumes
reverting systems with 117
deduplication
verifying space for before upgrading 38
disk firmware
understanding background updates for 172
Disk Qualification Package
when you need to update 108
disk shelves
how firmware updates are handled during Data ONTAP upgrades 172
disks
how firmware updates are handled during Data ONTAP upgrades 172
understanding background firmware updates for 172
verifying health of 34, 97, 114, 128, 143, 164
when you need to update the Disk Qualification Package for 108
disruptive downgrades
See downgrades
disruptive upgrades
definition of cluster 17
procedure for cluster 92
DNS
upgrade requirements for netgroups 28
documentation
how to receive automatic notification of changes to 181
how to send feedback about 181
downgrades
completing post-downgrade tasks 162
considerations for whether to manually update the SP firmware 133, 169
disruptive, performing 160
enabling and reverting LIFs to home ports, before and after 45, 101, 129, 148, 167
finding back-end configuration errors before downgrading 150
introduction to preparing features for 148
introduction to verifying the cluster is ready for 142
issues to know before performing cluster 140
nondisruptive, performing 153
obtaining Data ONTAP software images 55, 122, 152
overview of, to earlier release in same release family 138
performing nondisruptive cluster, using
OnCommand System Manager for 156
process for 152
requirements for MetroCluster configurations 140
requirements for planning 139
reviewing resources before performing 139
verifying MetroCluster configuration networking and storage status before 36, 98, 144, 165

D

Data ONTAP
overview of reversion to an earlier release family 109
overview of upgrade process 6
Data ONTAP Edge
recommendations for upgrading 175
upgrade overview 174
upgrade planning 18, 175
upgrade process overview 174
verifying system status after upgrade 178
Data ONTAP Edge software images
introduction to obtaining 176
Data ONTAP software images
command for installing on Data ONTAP Edge systems 177
obtaining 55, 122, 152

D
when to call technical support 138
workflow for cluster 138
downgrades, nondisruptive
two-node MetroCluster configurations, procedure for 89, 157
DQP
See Disk Qualification Package
dump backups
post-reversion considerations for 133
dump operations
verifying job status before upgrading or downgrading 42, 146
E
epsilon
effect on the upgrade sequence for four-node clusters 22
errors
finding before downgrading 150
expanding
aggregates to the 64-bit format 60
F
failover
LIF, verifying configuration of 39
failover groups
verifying before an upgrade 39
features
introduction to preparing for downgrade 148
introduction to preparing for reversion 116
preparing before upgrade 43
feedback
how to send comments about documentation 181
files
netgroup, verifying presence on all nodes before upgrade or revert 44, 116
firewall policies
verifying that IPv6 entries are restored after reverting 132
firmware
components that are updated automatically during Data ONTAP upgrades 172
considerations for whether to manually update the SP 133, 169
firmware updates
understanding background disk 172
Flash Cache
how firmware updates are handled during Data ONTAP upgrades 172
FlexCache volumes
removing before upgrade 52
FlexVol volumes
finding and removing 32-bit, after expanding aggregates to 64-bit 61
guarantee, enabling after upgrade to Data ONTAP 8.3 105
guarantees, converting from type file before upgrading to Data ONTAP 8.3 44
four-node clusters
how epsilon affects the upgrade sequence of 22
free space
ensuring adequate volume, prior to upgrades 35
FTP servers
 copying the Data ONTAP-v software image to 176
installing Data ONTAP-v software images from 177
G
groups
local UNIX, removing oversized names 43
guarantees
volume, converting from type file before upgrading to Data ONTAP 8.3 44
volume, enabling after upgrade to Data ONTAP 8.3 105
H
HA
See high availability
HA pairs
upgrading the first node using the rolling method 63
upgrading the first set of nodes using the batch method 74
upgrading the partner node using the rolling method 68
upgrading the set of partner nodes using the batch method 79
health
verifying storage 34, 97, 114, 128, 143, 164
high availability
verifying status of 32
HTTP servers
 copying the Data ONTAP-v software image to 176
installing Data ONTAP-v software images from 177
I
images
installing before a major upgrade 56
software, installing before a reversion 122
Infinite Volumes
considerations for reversion 112
considerations for upgrade 26
creating namespace mirror constituents after reverting 133, 134
creating namespace mirror constituents for tape backup after reverting 134
Infinite Volumes with storage classes
creating namespace mirror constituents after reverting 135
creating namespace mirror constituents for tape backup after reverting 136
information
how to send feedback about improving documentation 181
installing Data ONTAP software images from HTTP or FTP server 177
IP spaces
Cluster, deleting the system SVM 131
IPv4
configuring key management servers with Storage Encryption before reverting 116
IPv6
reconfiguring Storage Encryption for IPv4 before reverting 116
verifying connectivity for SVMs 98
IPv6 firewall entries
verifying they are restored after reverting 132
issues
cluster downgrade 140
reversion, for consideration before reverting 111

J
jobs
verifying status before upgrading or downgrading 42, 146

K
Kerberos
verifying configurations after upgrading 103
key management servers
configuring Storage Encryption for IPv4 before reverting 116

L
LDAP
configuring clients to use TLS 106
LIFs
disabling automatic rebalancing for 46
enabling and reverting to home ports 45, 101, 129, 148, 167
reenabling automatic rebalancing for 103
verifying sufficiency before upgrading 56
verifying the failover configuration for 39
limitations
cluster downgrade 140
reversion, for consideration before reverting 111
limits
verifying before a cluster upgrade 28
load-sharing mirrors
preparing for major upgrade 54
relocating after a major upgrade 102
local UNIX groups
removing oversized names 43
local UNIX users
removing oversized names 43
LUNs
ensuring adequate free space in volumes prior to upgrades 35

M
major upgrades
installing software images before 56
preparing SVM networking prior to 47
verifying networking after 104
verifying that SVMs can connect to external servers after 98
MCC
See MetroCluster configurations
MetroCluster configurations
downgrade requirements for 140
two-node, downgrading Data ONTAP for 89, 157
two-node, upgrading Data ONTAP for 89, 157
upgrade requirements for 27
verifying networking and storage status before upgrading or downgrading 36, 98, 144, 165
mirrors, load-sharing
preparing for major upgrade 54
relocating after a major upgrade 102
mixed version requirements
for cluster upgrades 21
mixed-format volumes
finding and removing after expanding aggregates to 64-bit 61

N
namespace constituents
order of upgrading nodes with 26
namespace mirror constituents
considerations for creating after reverting 112
creating for an Infinite Volume after reverting 134
creating for an Infinite Volume with storage classes after reverting 135
creating for tape backup of an Infinite Volume after reverting 134
creating for tape backup of an Infinite Volume with storage classes after reverting 136
order of upgrading nodes with 26
NDMP
considerations for avoiding interruptions during upgrades 171
NDUs
See nondisruptive upgrades
NetApp Support Site
introduction to obtaining Data ONTAP software images from 176
obtaining Data ONTAP Edge software images 174
obtaining Data ONTAP software images 55, 122, 152
netgroups
upgrade requirements 28
verifying file is present on all nodes before upgrade or revert 44, 116
networking
preparing SVM, for major upgrade 47
SVM considerations for major upgrades 23
verifying after a major upgrade 104
networking status
verifying MetroCluster configuration, before upgrading or downgrading 36, 98, 144, 165
NFS
protocol considerations for upgrades 171
setting desired NT ACL permissions display level 107
verifying client access for 131, 168
verifying Kerberos configurations after upgrading 103
nodes
order of upgrading for Infinite Volumes 26
planning sequence for batch upgrades 29
upgrading the first node in an HA pair using the rolling method 63
upgrading the first set of nodes in a batch of HA pairs using the batch method 74
upgrading the partner node in an HA pair using the rolling method 68
upgrading the set of partner nodes in a batch of HA pairs using the batch method 79
verifying netgroup file is present on all, before upgrade or revert 44, 116

nondisruptive downgrades
two-node MetroCluster configurations, procedure for 89, 157
using OnCommand System Manager for cluster 156
See also downgrades
non-disruptive upgrades
about optimizing service availability during 170
batch method for cluster 73
batch, planning sequence for 29
considerations for avoiding service interruptions during 170
guidelines for estimating the duration of 23
resuming SnapMirror operations after 102, 168
rolling upgrade method for 62
SnapMirror environment, steps for 54, 151
two-node MetroCluster configurations, procedure for 89, 157
types and methods of cluster 17
using automated method for cluster 85
using OnCommand System Manager for cluster 88

O
overview
downgrade to earlier release in same release family 138
upgrade process 6

P
partitioning
root-data, upgrade considerations for 25
performance baselines
establishing with Perfstat before upgrade 30
performing upgrades
introduction to, for cluster software 62
Perfstat
creating performance baseline with, before upgrading 30
permissions
setting desired NT ACL display level for NFS clients 107
planning
requirements for downgrades 139
reversions for clusters that contain Infinite Volumes 112
reversions, introduction to 110
upgrades 20
upgrades for clusters that contain Infinite Volumes 26
upgrades with Upgrade Advisor 19

P
overview
downgrade to earlier release in same release family 138
upgrade process 6

R
release families
impact of upgrades on service availability 170
release requirements
for cluster upgrades 21
requirements
downgrade planning 139
for cluster upgrades 21
MetroCluster configuration downgrade 140
MetroCluster configuration upgrade 27
SnapMirror upgrade 25
verifying job status before upgrading or downgrading 42, 146
resources
reviewing before downgrading 139
reviewing before upgrading 21, 110
restore operations
verifying job status before upgrading or downgrading 42, 146
reversion issues
considerations before reverting 111
considerations for Infinite Volumes 112
verifying that IPv6 firewall entries are restored 132
reversions
enabling and reverting LIFs to home ports, after 45, 101, 129, 148, 167
installing software images prior to 122
introduction to completing tasks after finishing 126
introduction to planning for 110
introduction to preparing features for 116
introduction to preparing for cluster 113
introduction to requirements for cluster 111
introduction to verifying the cluster is ready for 113
obtaining Data ONTAP software images 55, 122, 152
procedure for cluster 124
SnapMirror requirements for 111
workflow for cluster 109
reversions, cluster
overview of 109
reverting
systems that have the SP automatic configuration enabled 120
systems with compressed volumes 118
systems with deduplicated volumes 117
reverting to a previous release
issues and limitations to consider before 111
preparing Snapshot copies after 131
preparing Snapshot copies before 120
when to call technical support 109
reverts
considerations for whether to manually update the
SP firmware 133, 169
verifying that netgroup file is present on all nodes before 44, 116
rolling upgrades
definition of nondisruptive cluster 17
process for 62
upgrading the first node in an HA pair 63
upgrading the partner node in an HA pair 68
verifying cluster version 95
root-data partitioning
upgrade considerations for 25

S
SAN
ensuring adequate space in volumes prior to upgrades 35
protocol considerations for upgrades 171
verifying configuration after upgrade 103
verifying configuration prior to upgrade 41
servers
copying the Data ONTAP-v software image to HTTP or FTP 176
service availability
about optimizing during upgrades 170
considerations for avoiding interruptions during upgrades 170
impact of upgrades on 170
Service Processors
See SPs
session-oriented protocols
considerations for avoiding service interruptions during upgrades 171
single-node clusters
upgrading disruptively 92
SnapDiff
reenabling for a reverted Infinite Volume 134
reenabling for a reverted Infinite Volume with storage classes 136
SnapMirror environments
identifying destination volumes 174
resuming operations after NDU 102, 168
reversion requirements for 111
upgrade requirements for 25
upgrading nondisruptively 54, 151
Snapshot copies
deleting before reverting systems with compressed data 118
finding and removing 32-bit, after expanding aggregates to 64-bit 61
preparing after reverting 131
preparing before reverting 120
upgrade planning 174
SnapVault environments
reversion requirements for 111
software images
command for installing on Data ONTAP Edge systems 177
copying 176
Data ONTAP-v, copying from the HTTP or FTP server to the storage system 176
installing before a major upgrade 56
installing before a reversion 122
installing Data ONTAP-v, from HTTP or FTP servers 177
introduction to obtaining for Data ONTAP Edge 176
obtaining 55, 122, 152
software update command
for installing software images on Data ONTAP Edge systems 177
SPs
considerations for whether to manually update the firmware 133, 169
how firmware updates are handled during Data ONTAP upgrades 172
reverting systems that have the automatic configuration enabled 120
SSL
configuring LDAP clients to use TLS instead 106
stateless protocols
avoiding service interruptions during upgrades 171
status
verifying disk, aggregate, and volume 34, 97, 114, 128, 143, 164
storage
verifying health 34, 97, 114, 128, 143, 164
storage classes
creating namespace mirror constituents for a reverted Infinite Volume with 133, 135
reenabling SnapDiff for a reverted Infinite Volume with 136
Storage Encryption
configuring with IPv4 key management servers before reverting 116
storage failover
verifying status of 32
storage status
verifying MetroCluster configuration, before upgrading or downgrading 36, 98, 144, 165
storage systems
compatibility with Data ONTAP 174
storage systems using array LUNs
finding errors before downgrading 150
suggestions
how to send feedback about documentation 181
support
when to call during downgrade 138
when to call during revert 109
SVMs
major upgrade networking considerations for 23
preparing networking for a major upgrade 47
system, deleting for the Cluster IP space 131
verifying IPv6 connectivity to external servers 98
verifying networking for, before upgrading 56
verifying that netgroup file is present on all nodes before upgrade or revert 44, 116
system files
  Data ONTAP-v, copying software image to HTTP or FTP servers 176
  Data ONTAP-v, installing 177
system firmware
  components that are updated automatically during Data ONTAP upgrades 172
system limits
  verifying before a cluster upgrade 28
system status
  verifying Data ONTAP Edge, after upgrade 178
system time
  verifying 41, 115, 146

T
tape backup and restore
  creating namespace mirror constituents for Infinite Volumes after reverting 134
  creating namespace mirror constituents for Infinite Volumes with storage classes after reverting 136
tasks
  introduction to completing post-reversion 126
technical support
  when to call during downgrade 138
  when to call during revert 109
TLS
  configuring LDAP clients to use 106
troubleshooting
  reverting LIFs to home ports 45, 101, 129, 148, 167
Twitter
  how to receive automatic notification of documentation changes 181
two-node MetroCluster configurations
  downgrading Data ONTAP for 89, 157
  upgrading Data ONTAP for 89, 157

U
UNIX
  removing oversized local user and group names 43
  understanding background disk firmware 172
  enabling volume guarantees after 105
Upgrade Advisor tool
  planning your upgrade with 19
upgrades
  about maintaining service availability during 170
  batch, planning sequence for 29
  checklist for 7
  considerations for avoiding service interruptions 170
  considerations regarding 32-bit data 25
  considerations with session-oriented protocols 171
  considerations with stateless protocols 171
  creating performance baseline before 30
  disabling 32-bit capability before performing cluster 59
  enabling and reverting LIFs to home ports, before and after 45, 101, 129, 148, 167
  ensuring adequate volume space prior to 35
  firmware components that are updated automatically during Data ONTAP cluster 172
  guidelines for estimating the duration of 23
  how epsilon affects sequence of four-node cluster 22
  impact on service availability 170
  introduction to performing cluster software 62
  introduction to requirements for cluster 21
  major, installing software images before 56
  major, SVM networking considerations for 23
  major, verifying networking after 104
  obtaining Data ONTAP software images 55, 122, 152
  performing nondisruptive cluster, using automated method 85
  performing nondisruptive cluster, using OnCommand System Manager for 88
planning for 20
  planning with Upgrade Advisor 19
preparation for 31
  preparing for Data ONTAP Edge system 175
procedure for disruptive cluster 92
process for nondisruptive batch method for cluster 73
process overview 6
recommendations for Data ONTAP Edge systems 175
reenabling automatic LIF rebalancing after batch 103
removing FlexCache volumes before 52
requirements for cluster 21
  requirements for MetroCluster configurations 27
  requirements for netgroups 28
  requirements for SnapMirror 25
reviewing resources before performing 21, 110
root-data partitioning considerations for 25
SnapMirror environment, nondisruptive steps 54, 151
  types of nondisruptive and disruptive cluster 17
  upgrading the first node in an HA pair using the rolling method 63
  upgrading the first set of nodes in a batch of HA pairs using the batch method 74
  upgrading the partner node in an HA pair using the rolling method 68
  upgrading the set of partner nodes in a batch of HA pairs using the batch method 79
  verifying cluster version 95
  verifying LIF failover configuration for 39
  verifying limits for cluster 28
  verifying MetroCluster configuration networking and storage status before 36, 98, 144, 165
  verifying NFS Kerberos configurations after 103
  verifying SAN configuration after 103
  verifying SAN configuration prior to 41
  verifying system status after Data ONTAP Edge upgrade 178
  verifying that netgroup file is present on all nodes before 44, 116
  verifying the cluster is ready for 31
upgrades, cluster workflow for 6
upgrades, nondisruptive
  rolling upgrade method for 62
two-node MetroCluster configurations, procedure for
89, 157
upgrades, rolling
  process for 62
users
  local UNIX, removing oversized names 43
utilities
  checking for common configuration errors with
  Config Advisor 31, 32
downloading and running Config Advisor 31, 32

V
volumes
  deduplicated, verifying space for 38
  ensuring adequate space, prior to upgrades 35
  finding and removing 32-bit and mixed-format, after
  expanding aggregates to 64-bit 61
  FlexCache, removing before upgrade 52
  guarantees, converting from type file before
  upgrading to Data ONTAP 8.3 44
  reverting systems with compressed 118
  verifying health of 34, 97, 114, 128, 143, 164
  verifying volume status before upgrading or
downgrading 42, 146
Vservers
  See SVMs

W
workflows
  for cluster downgrades 138
  for cluster reversions 109
  for cluster upgrades 6