



What should I verify before I upgrade with or without Upgrade Advisor?

ONTAP 9

NetApp
November 10, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/upgrade/task_what_to_check_before_upgrade.html on November 10, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- What should I verify before I upgrade with or without Upgrade Advisor? 1
 - What to check before upgrading 1
 - Verify cluster health 1
 - Verify storage health 2
 - Verify SVM routing configuration 3
 - Verifying the LIF failover configuration 3
 - Verify status 5
 - Verify all LIFS are on home ports before upgrade 6
 - Use Active IQ Config Advisor to verify there are no common configuration errors 8
 - Special considerations 9

What should I verify before I upgrade with or without Upgrade Advisor?

What to check before upgrading

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

Verify cluster health

Before you upgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

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

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

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

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

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

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
Time                      Node      Severity      Event
-----
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Related information

[System administration](#)

Verify storage health

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

1. Verify disk status:

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

2. Verify that all aggregates are online by displaying the state:

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

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

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

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

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

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

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

4. Verify that there are no inconsistent volumes:

```
volume show -is-inconsistent true
```

See the Knowledge Base article [Volume Showing WAFL Inconsistent](#) on how to address the inconsistent volumes.

Related information

[Logical storage management](#)

Verify SVM routing configuration

It is a best practice to configure one default route for an SVM. To avoid disruption, you should ensure that the default route is able to reach any network address that is not reachable by a more specific route. For more information, see [SU134: Network access might be disrupted by incorrect routing configuration in clustered ONTAP](#).

The routing table for an SVM determines the network path the SVM uses to communicate with a destination. It's important to understand how routing tables work so that you can prevent network problems before they occur.

Routing rules are as follows:

- ONTAP routes traffic over the most specific available route.
- ONTAP routes traffic over a default gateway route (having 0 bits of netmask) as a last resort, when more specific routes are not available.

In the case of routes with the same destination, netmask, and metric, there is no guarantee that the system will use the same route after a reboot or after an upgrade. This is especially an issue if you have configured multiple default routes.

Verifying the LIF failover configuration

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



During the upgrade process, LIFs are migrated based on the upgrade method. Depending upon the upgrade method, the LIF failover policy might or might not be used.

If you have 8 or more nodes in your cluster, the automated upgrade is performed using the batch method. The batch upgrade method involves dividing the cluster into multiple upgrade batches, upgrading the set of nodes in the first batch, upgrading their high-availability (HA) partners, and then repeating the process for the remaining batches. In ONTAP 9.7 and earlier, if the batch method is used, LIFs are migrated to the HA partner of the node being upgraded. In ONTAP 9.8 and later, if the batch method is used, LIFs are migrated to the other batch group.

If you have less than 8 nodes in your cluster, the automated upgrade is performed using the rolling method. The rolling upgrade method involves initiating a failover operation on each node in an HA pair, updating the "failed" node, initiating giveback, and then repeating the process for each HA pair in the cluster. If the rolling method is used, LIFs are migrated to the failover target node as defined by the LIF failover policy.

1. Display the failover policy for each data LIF:

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

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

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

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

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

2. If the failover policy is set to disabled for any LIFs, other than SAN LIFs, use the network interface modify command to enable failover.
3. For each LIF, verify that the **Failover Targets** field includes data ports from a different node that will remain up while the LIF's home node is being upgraded.

You can use the network interface failover-groups modify command to add a failover target to the failover group.

Example

```
network interface failover-groups modify -vserver vs0 -failover-group  
fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

Related information

[Network and LIF management](#)

Verify status

Before you upgrade, you should verify the following:

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

Verifying HA status

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

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

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

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

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

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

2 entries were displayed.

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

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

This example shows that cluster HA is configured:

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

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

Verifying LDAP status (ONTAP 9.2 and later)

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

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

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

Verifying DNS server status (ONTAP 9.2 and later)

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

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

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

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

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

Verify all LIFs are on home ports before upgrade

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

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

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

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


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

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

8 entries were displayed.

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

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

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

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

This command reverts all LIFs back to their home ports.

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

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

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

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

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
vs0					
true	data001	up/up	192.0.2.120/24	node0	e0e
true	data002	up/up	192.0.2.121/24	node0	e0f
true	data003	up/up	192.0.2.122/24	node0	e2a
true	data004	up/up	192.0.2.123/24	node0	e2b
true	data005	up/up	192.0.2.124/24	node1	e0e
true	data006	up/up	192.0.2.125/24	node1	e0f
true	data007	up/up	192.0.2.126/24	node1	e2a
true	data008	up/up	192.0.2.127/24	node1	e2b

8 entries were displayed.

Use Active IQ Config Advisor to verify there are no common configuration errors

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

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



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

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

Special considerations

Pre-upgrade checks

Depending on your environment, you need to consider certain factors before you start your upgrade. Get started by reviewing the table below to see what special considerations you need to consider.

Ask yourself...	If your answer is yes, then do this...
Do I have a mixed version cluster?	Check mixed version requirements
Do I have a SAN configuration?	Verify the SAN configuration
Do I have a MetroCluster configuration?	<ul style="list-style-type: none">• Review specific upgrade requirements for MetroCluster configurations• Verify networking and storage status
Are nodes on my cluster using root-data partitioning and root-data-data-partitioning?	Examine upgrade considerations for root-data and root-data-data partitioning
Do I have deduplicated volumes and aggregates?	Verify you have enough free space for your deduplicated volumes and aggregates
Is my cluster running SnapMirror?	<ul style="list-style-type: none">• Review upgrade requirements for SnapMirror• Prepare your SnapMirror relationships for upgrade
Is my cluster running SnapLock?	Review upgrade considerations for SnapLock
Am I upgrading from ONTAP 8.3 and have load-sharing mirrors?	Prepare all load-sharing mirrors for upgrade
Am I using NetApp Storage Encryption with external key management servers?	Delete any existing key management server connections
Do I have netgroups loaded into SVMs?	Verify that the netgroup file is present on each node
Do I have LDAP clients using SSLv3?	Configure LDAP clients to use TLS
Am I using session-oriented protocols?	Review considerations for session-oriented protocols
Is SSL FIPS mode enabled on a cluster where administrator accounts authenticate with an SSH public key?	Review requirements for SSH public keys

Mixed version requirements

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

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

nodes.

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

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

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

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

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

Verifying the SAN configuration

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

1. On each host, verify that a sufficient number of direct and indirect paths are configured, and that each path is active.

Each host must have a path to each node in the cluster.

2. Verify that each host is connected to a LIF on each node.

You should record the list of initiators for comparison after the upgrade.

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

MetroCluster configurations

Upgrade requirements for MetroCluster configurations

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

Required methods for performing major and minor upgrades of MetroCluster configurations

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

Beginning with ONTAP 9.3, major upgrades to MetroCluster configurations can be performed with automatic non-disruptive upgrade (NDU) procedure. On systems running ONTAP 9.2 or earlier, major upgrades to MetroCluster configurations must be performed with the NDU procedure that is specific to MetroCluster configurations.

General requirements

- Both clusters must be running the same version of ONTAP.

You can verify the ONTAP version by using the version command.

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



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

- For all configurations except two-node clusters, you can nondisruptively upgrade both clusters at the same time.

For nondisruptive upgrade in two-node clusters, the clusters must be upgraded one node at a time.

- The aggregates in both clusters must not be in resyncing RAID status.

During MetroCluster healing, the mirrored aggregates are resynchronized. You can verify if the MetroCluster configuration is in this state by using the `storage aggregate plex show -in-progress true` command. If any aggregates are being synchronized, you should not perform an upgrade until the resynchronization is complete.

- Negotiated switchover operations will fail while the upgrade is in progress.

To avoid issues with upgrade or revert operations, do not attempt an unplanned switchover during an upgrade or revert operation unless all nodes on both clusters are running the same version of ONTAP.

Configuration requirements for normal operation

- The source SVM LIFs must be up and located on their home nodes.

Data LIFs for the destination SVMs are not required to be up or to be on their home nodes.

- All aggregates at the local site must be online.
- All root and data volumes owned by the local cluster's SVMs must be online.

Configuration requirements for switchover

- All LIFs must be up and located on their home nodes.
- All aggregates must be online, except for the root aggregates at the DR site.

Root aggregates at the DR site are offline during certain phases of switchover.

- All volumes must be online.

Related information

[Verifying networking and storage status for MetroCluster configurations](#)

Verify networking and storage status for MetroCluster configurations

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

1. Verify the LIF status: `network interface show`

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

```

cluster1::> network interface show

```

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

```

27 entries were displayed.

```

2. Verify the state of the aggregates: `storage aggregate show -state !online`

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

This example shows a cluster in normal operation:

```

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

```

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

```

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

```

3. Verify the state of the volumes: `volume show -state !online`

This command displays any volumes that are *not* online.

If the MetroCluster configuration is in normal operation (it is not in switchover state), the output should show all volumes owned by the cluster's secondary SVMs (those with the SVM name appended with "-mc").

Those volumes come online only in the event of a switchover.

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


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

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

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

Related information

[Upgrade requirements for MetroCluster configurations](#)

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

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

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

Related information

[ONTAP concepts](#)

Verify that deduplicated volumes and aggregates contain sufficient free space

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

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

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

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

Logical storage management

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

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

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

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

Disk and aggregate management

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

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

SnapMirror

Upgrade requirements for SnapMirror

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

- If you are upgrading clusters with DP SnapMirror relationships, you must upgrade the destination cluster/nodes before you upgrade the source cluster/nodes.

- Before upgrading a cluster that is running SnapMirror, SnapMirror operations must be quiesced for each node that contains destination volumes, and each peered SVM must have a unique name across the clusters.

To prevent SnapMirror transfers from failing, you must suspend SnapMirror operations and, in some cases, upgrade destination nodes before upgrading source nodes. The following table describes the two options for suspending SnapMirror operations.

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

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

Related information

[ONTAP concepts](#)

Prepare SnapMirror relationships for a nondisruptive upgrade

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

1. Use the `snapmirror show` command to determine the destination path for each SnapMirror relationship.

2. For each destination volume, suspend future SnapMirror transfers: `snapmirror quiesce -destination-path destination`

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

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

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

3. Verify that all SnapMirror relationships are quiesced: `snapmirror show -status !Quiesced`

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

This example shows that all SnapMirror relationships are quiesced:

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

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

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

Related information

[Upgrade requirements for SnapMirror](#)

Upgrade considerations for SnapLock

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

Prepare all load-sharing mirrors for a major upgrade

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

of ONTAP.

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

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

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

Delete existing external key management server connections before upgrading

If you are using NetApp Storage Encryption (NSE) on ONTAP 9.2 or earlier and upgrading to ONTAP 9.3 or later, you must use the command line interface (CLI) to delete any existing external key management (KMIP) server connections before performing the upgrade.

1. Verify that the NSE drives are unlocked, open, and set to the default manufacture secure ID 0x0:

```
storage encryption disk show -disk*
```

2. Enter the advanced privilege mode:

```
set -privilege advanced
```

3. Use the default manufacture secure ID 0x0 to assign the FIPS key to the self-encrypting disks (SEDs):

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

4. Verify that assigning the FIPS key to all disks is complete: `storage encryption disk show-status`

5. Verify that the **mode** for all disks is set to **data**: `storage encryption disk show`

6. View the configured KMIP servers: `security key-manager show`

7. Delete the configured KMIP servers: `security key-manager delete -address kmip_ip_address`

8. Delete the external key manager configuration: `security key-manager delete-kmip-config`



This step does not remove the NSE certificates.

After the upgrade is complete, you must reconfigure the KMIP server connections.

Related information

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

Verifying that the netgroup file is present on all nodes

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

[NFS management](#) contains more information about netgroups and loading them from a URI.

1. Set the privilege level to advanced: `set -privilege advanced`
2. Display the netgroup status for each SVM: `vserver services netgroup status`
3. Verify that for each SVM, each node shows the same netgroup file hash value: `vserver services name-service netgroup status`

If this is the case, you can skip the next step and proceed with the upgrade or revert. Otherwise, proceed to the next step.

4. On any one node of the cluster, manually load the netgroup file: `vserver services netgroup load -vserver vserver_name -source uri`

This command downloads the netgroup file on all nodes. If a netgroup file already exists on a node, it is overwritten.

Configure LDAP clients to use TLS for highest security

Before upgrading to the target ONTAP release, you must configure LDAP clients using SSLv3 for secure communications with LDAP servers to use TLS. SSL will not be available after the upgrade.

By default, LDAP communications between client and server applications are not encrypted. You must disallow the use of SSL and enforce the use of TLS.

1. Verify that the LDAP servers in your environment support TLS.

If they do not, do not proceed. You should upgrade your LDAP servers to a version that supports TLS.

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

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

3. For each LDAP client configuration, disallow SSL to enforce the use of TLS: `vserver services name-service ldap client modify -vserver vserver_name -client-config ldap_client_config_name -allow-ssl false`
4. Verify that the use of SSL is no longer allowed for any LDAP clients: `vserver services name-service ldap client show`

Related information

[NFS management](#)

Considerations for session-oriented protocols

Clusters and session-oriented protocols might cause adverse effects on clients and applications in certain areas during upgrades.

If you are using session-oriented protocols, consider the following:

- SMB

If you serve continuously available (CA) shares with SMBv3, you can use the automated nondisruptive upgrade method (with System Manager or the CLI), and no disruption is experienced by the client.

If you are serving shares with SMBv1 or SMBv2, or non-CA shares with SMBv3, client sessions are disrupted during upgrade takeover and reboot operations. You should direct users to end their sessions before you upgrade.

For more information, see [TR-4100: Nondisruptive Operations with SMB File Shares ONTAP 9.x](#).

Hyper-V and SQL Server over SMB support nondisruptive operations (NDOs). If you configured a Hyper-V or SQL Server over SMB solution, the application servers and the contained virtual machines or databases remain online and provide continuous availability during the ONTAP upgrade.

- NFSv4.x

NFSv4.x clients will automatically recover from connection losses experienced during the upgrade using normal NFSv4.x recovery procedures. Applications might experience a temporary I/O delay during this process.

- NDMP

State is lost and the client user must retry the operation.

- Backups and restores

State is lost and the client user must retry the operation.



Do not initiate a backup or restore during or immediately before an upgrade. Doing so might result in data loss.

- Applications (for example, Oracle or Exchange)

Effects depend on the applications. For timeout-based applications, you might be able to change the timeout setting to longer than the ONTAP reboot time to minimize adverse effects.

Considerations for session-oriented protocols

If SSL FIPS mode is enabled on a cluster where administrator accounts authenticate with an SSH public key, you must ensure that the host key algorithm is supported on the target release before upgrading ONTAP.

Note: Host key algorithm support has changed in ONTAP 9.11.1 and later releases.

ONTAP release	Supported key types	Unsupported key types
---------------	---------------------	-----------------------

9.11.1 and later	ecdsa-sha2-nistp256	rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ssh-dss ssh-rsa

Existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type before enabling upgrading, or administrator authentication will fail.

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

Copyright information

Copyright © 2022 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

Trademark information

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