What should I do after my upgrade?

ONTAP 9

NetApp
August 12, 2022

Table of Contents

What should I do after my upgrade?

What to do after upgrading

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

Post-upgrade cluster verification

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

Before you begin

If you are using a MetroCluster FC configuration, you also need to verify that the cluster is enabled for automatic unplanned switchover.

Verify cluster version

After all of the HA pairs have been upgraded, you must use the version command to verify that all of the nodes are running the target release.

The cluster version is the lowest version of ONTAP running on any node in the cluster. If the cluster version is not the target ONTAP release, you can upgrade your cluster.

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

   ```
   version
   ```

2. If the cluster version is not the target ONTAP release, you can verify the upgrade status of all nodes:

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

Verify cluster health

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

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

   ```
   cluster show
   ```

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

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

2. Set the privilege level to advanced:

   `set -privilege advanced`

   Enter “y” to continue.

3. Verify the configuration details for each RDB process.

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

     Note that each ring might have a different quorum master.

To display this RDB process…	Enter this command…
Management application	`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`

   This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. 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 that automatic unplanned switchover is enabled

After you upgrade a cluster, you should verify that automatic unplanned switchover is enabled.

About this task

This procedure is performed only for MetroCluster FC configurations. If you are using a MetroCluster IP configuration, skip this procedure.

Steps

1. Check whether automatic unplanned switchover is enabled:

   `metrocluster show`

   If automatic unplanned switchover is enabled, the following statement appears in the command output:

   ```
   AUSO Failure Domain  auso-on-cluster-disaster
   ```

2. If the statement does not appear, enable an automatic unplanned switchover:

   `metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster`

3. Verify that an automatic unplanned switchover has been enabled by repeating Step 1.

Verify storage health

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	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.

   ```
   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

Disk and aggregate management

Verify all LIFS are on home ports after upgrade

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

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

1. Display the status of all LIFs: `network interface show -fields home-ports,curr-port`

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

```
cluster1::> network interface show -fields home-port,curr-port
vserver                           lif       home-port curr-port
--------------------------------- --------- --------- ---------
C1_sti96-vsim-ucs539g_1622463615 clus_mgmt e0d       e0d
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539g_cluster_mgmt_inet6
e0d e0d
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539g_mgmt1 e0c e0c
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539g_mgmt1_inet6 e0c e0c
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539h_cluster_mgmt_inet6
e0d e0d
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539h_mgmt1 e0c e0c
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539h_mgmt1_inet6 e0c e0c
Cluster                           sti96-vsim-ucs539g_clus1 e0a e0a
Cluster                           sti96-vsim-ucs539g_clus2 e0b e0b
Cluster                           sti96-vsim-ucs539h_clus1 e0a e0a
Cluster                           sti96-vsim-ucs539h_clus2 e0b e0b
vs0                               sti96-vsim-ucs539g_data1 e0d e0d
vs0                               sti96-vsim-ucs539g_data1_inet6 e0d e0d
vs0                               sti96-vsim-ucs539g_data2 e0e e0e
vs0                               sti96-vsim-ucs539g_data2_inet6 e0e e0e
vs0                               sti96-vsim-ucs539g_data3 e0f e0f
vs0                               sti96-vsim-ucs539g_data3_inet6 e0f e0f
vs0                               sti96-vsim-ucs539g_data4 e0d e0d
vs0                               sti96-vsim-ucs539g_data4_inet6 e0d e0d
vs0                               sti96-vsim-ucs539g_data5 e0e e0e
vs0                               sti96-vsim-ucs539g_data5_inet6 e0e e0e
vs0                               sti96-vsim-ucs539g_data6 e0f e0f
vs0                               sti96-vsim-ucs539g_data6_inet6 e0f e0f
vs0                               sti96-vsim-ucs539h_data1 e0d e0d
vs0                               sti96-vsim-ucs539h_data1_inet6 e0d e0d
vs0                               sti96-vsim-ucs539h_data2 e0e e0e
vs0                               sti96-vsim-ucs539h_data2_inet6 e0e e0e
vs0                               sti96-vsim-ucs539h_data3 e0f e0f
vs0                               sti96-vsim-ucs539h_data3_inet6 e0f e0f
vs0                               sti96-vsim-ucs539h_data4 e0d e0d
vs0                               sti96-vsim-ucs539h_data4_inet6 e0d e0d
vs0                               sti96-vsim-ucs539h_data5 e0e e0e
vs0                               sti96-vsim-ucs539h_data5_inet6 e0e e0e
vs0                               sti96-vsim-ucs539h_data6 e0f e0f
vs0                               sti96-vsim-ucs539h_data6_inet6 e0f e0f
35 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
         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
         data002    up/up      192.0.2.121/24   node0    e0f     true
         data003    up/up      192.0.2.122/24   node0    e2a     true
         data004    up/up      192.0.2.123/24   node0    e2b     true
         data005    up/up      192.0.2.124/24   node1    e0e     true
         data006    up/up      192.0.2.125/24   node1    e0f     true
         data007    up/up      192.0.2.126/24   node1    e2a     true
         data008    up/up      192.0.2.127/24   node1    e2b     true
8 entries were displayed.
```

Verify special configurations

Post upgrade checks for special configurations

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

Ask yourself…	If your answer is yes, then do this…
Did I upgrade to ONTAP 9.8 or later from ONTAP 9.7 or earlier	Verify your network configuration
Do I have a MetroCluster configuration?	Verify your networking and storage status

Ask yourself…	If your answer is yes, then do this…
Do I have a SAN configuration?	Verify your SAN configuration
Am I using NetApp Storage Encryption and I upgraded to ONTAP 9.3 or later?	Reconfigure KMIP server connections
Do I have load-sharing mirrors?	Relocate moved load-sharing mirror source volumes
Am I using SnapMirror?	Resume SnapMirror operations
Did I upgrade from ONTAP 8.3.0?	Set the desired NT ACL permissions display level for NFS clients
Do I have administrator accounts created prior to ONTAP 9.0?	Enforce SHA-2 on administrator passwords
Do I have user accounts for Service Processor (SP) access created prior to ONTAP 9.9.1?	Verify the change in accounts that can access the Service Processor

Verifying your network configuration after upgrade

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

1. Verify each port has reachability to its expected domain:`network port reachability show -detail`

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

Verify networking and storage status for MetroCluster configurations

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

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

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

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            cluster1-a1_clus1
                         up/up    192.0.2.1/24       cluster1-01
                                                                  e2a
true
            cluster1-a1_clus2
                         up/up    192.0.2.2/24       cluster1-01
                                                                  e2b
true


cluster1-01
            clus_mgmt    up/up    198.51.100.1/24    cluster1-01
                                                                  e3a
true
            cluster1-a1_inet4_intercluster1
                         up/up    198.51.100.2/24    cluster1-01
                                                                  e3c
true
            ...

27 entries were displayed.
```

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

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

   This example shows a cluster in normal operation:

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

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

```
cluster1::> storage aggregate show -state !online
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b1
                0B        0B    0% offline      0 cluster2-01
raid_dp,

mirror

degraded
aggr0_b2
                0B        0B    0% offline      0 cluster2-02
raid_dp,

mirror

degraded
2 entries were displayed.
```

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

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

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

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

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

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

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

   See the Knowledge Base article Volume Showing WAFL Inconsistent on how to address the inconsistent volumes.

Verify the SAN configuration after an upgrade

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

1. Verify that each initiator is connected to the correct LIF.

   You should compare the list of initiators to the list you made during the upgrade preparation.

For…	Enter…
iSCSI	`iscsi initiator show -fields igroup,initiator-name,tpgroup`
FC	`fcp initiator show -fields igroup,wwpn,lif`

Reconfiguring KMIP server connections after upgrading to ONTAP 9.3 or later

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

1. Configure the key manager connectivity:`security key-manager setup`
2. Add your KMIP servers: `security key-manager add -address key_management_server_ip_address`
3. Verify that KMIP servers are connected: `security key-manager show -status`
4. Query the key servers: `security key-manager query`
5. Create a new authentication key and passphrase: `security key-manager create-key -prompt -for-key true`

   The passphrase must have a minimum of 32 characters.
6. Query the new authentication key: `security key-manager query`
7. Assign the new authentication key to your self-encrypting disks (SEDs): `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   Make sure you are using the new authentication key from your query.
8. If needed, assign a FIPS key to the SEDs: `storage encryption disk modify -disk disk_id -fips-key-id fips_authentication_key_id`

   If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

Relocating moved load-sharing mirror source volumes

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

1. Identify the location to which you are moving the load-sharing mirror source volume by using the record you created before moving the load-sharing mirror source volume.
2. Move the load-sharing mirror source volume back to its original location by using the volume move start command.

Resuming SnapMirror operations

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

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

1. Resume transfers for each SnapMirror relationship that was previously quiesced: `snapmirror resume *`

   This command resumes the transfers for all quiesced SnapMirror relationships.
2. Verify that the SnapMirror operations have resumed: `snapmirror show`

```
cluster1::> snapmirror show

Source            Destination  Mirror  Relationship  Total
Last
Path        Type  Path         State   Status        Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
cluster1-vs1:dp_src1
            DP   cluster1-vs2:dp_dst1
                              Snapmirrored
                                      Idle           -         true    -
cluster1-vs1:xdp_src1
            XDP  cluster1-vs2:xdp_dst1
                              Snapmirrored
                                      Idle           -         true    -
cluster1://cluster1-vs1/ls_src1
            LS   cluster1://cluster1-vs1/ls_mr1
                              Snapmirrored
                                      Idle           -         true    -
                 cluster1://cluster1-vs1/ls_mr2
                              Snapmirrored
                                      Idle           -         true    -
4 entries were displayed.
```

For each SnapMirror relationship, verify that the Relationship Status is **Idle**. If the status is **Transferring**, wait for the SnapMirror transfer to complete, and then reenter the command to verify that the status has changed to **Idle**.

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

Setting the desired NT ACL permissions display level for NFS clients

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

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

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

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

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

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

Enforcing SHA-2 on administrator account passwords

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

The password hash functionality enables you to do the following:

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

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

Manageability enhancements

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

      Doing so forces MD5 account users to change their passwords upon next login.

   b. Ask users of MD5 accounts to log in through a console or SSH session.

      The system detects that the accounts are expired and prompts users to change their passwords. SHA-512 is used by default for the changed passwords.

2. For MD5 accounts whose users do not log in to change their passwords within a period of time, force the account migration:
   a. Lock accounts that still use the MD5 hash function (advanced privilege level): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

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

b. Unlock the accounts when the users are ready to change their passwords: `security login unlock -vserver vserver_name -username user_name`

c. Have users log in to their accounts through a console or SSH session and change their passwords when the system prompts them to do so.

Change in user accounts that can access the Service Processor

If you created user accounts in ONTAP 9.8 and earlier releases that can access the Service Processor (SP) with a non-admin role and you upgrade to ONTAP 9.9.1 or later, any non-admin value in the `-role` parameter is modified to `admin`.

For more information, see Accounts that can access the SP.

When you need to update the Disk Qualification Package

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

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

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

  For example, if you already have 1-TB drives and add 2-TB drives, you need to check for the latest DQP update.

- Whenever you update the disk firmware
- Whenever newer disk firmware or DQP files are available
- Whenever you upgrade to a new version of ONTAP.

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

Related information

NetApp Downloads: Disk Qualification Package

NetApp Downloads: Disk Drive Firmware