NetApp

Verify special configurations

ONTAP 9

NetApp
March 09, 2022

Table of Contents

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
Do I have a SAN configuration?	Verify your SAN configuration
Am I using NetApp Storage Encryption and I upgraded to ONTAP 9.3 or later?	Reconfigure KMIP server connections
Do I have load-sharing mirrors?	Relocate moved load-sharing mirror source volumes
Am I using SnapMirror?	Resume SnapMirror operations
Did I upgrade from ONTAP 8.3.0?	Set the desired NT ACL permissions display level for NFS clients
Do I have administrator accounts created prior to ONTAP 9.0?	Enforce SHA-2 on administrator passwords

Verifying your network configuration after upgrade

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

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

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

Verify networking and storage status for MetroCluster configurations

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

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

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

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


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

27 entries were displayed.
```

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

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

   This example shows a cluster in normal operation:

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

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

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

mirror

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

mirror

degraded
2 entries were displayed.
```

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

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

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

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

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

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

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

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

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.