What should I do after reverting my cluster?

ONTAP 9

NetApp
May 18, 2021

Table of Contents

Things to verify after revert . . . 1
- Verify cluster and storage health after downgrade or revert . . . 1
- Enable automatic switchover for MetroCluster configurations . . . 3
- Enable and revert LIFs to home ports after a revert . . . 4
- Enable Snapshot copy policies after reverting . . . 5
- Verify client access (CIFS and NFS) . . . 6
- Verify IPv6 firewall entries . . . 6
- Revert password hash function to the supported encryption type . . . 7
- Considerations for whether to manually update the SP firmware . . . 8

Things to verify after revert

After you revert, there are various tasks you need to perform to verify that your cluster is ready.

Verify cluster and storage health after downgrade or revert

After you downgrade or revert a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum. You should also verify the status of your disks, aggregates, and volumes.

Verify cluster health

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`
3. Enter `y` to continue.
4. 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.
```

1. 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.

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

2. Return to the admin privilege level: `set -privilege admin`

Related information

System administration

Verify storage health

After you revert or downgrade 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.

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.

   ```
   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`

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

Related information

Disk and aggregate management

Enable automatic switchover for MetroCluster configurations

This topic provides information regarding the additional tasks that you must perform after the reversion of MetroCluster configurations.

1. Enable automatic unplanned switchover: `metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster`
2. Validate the MetroCluster configuration: `metrocluster check run`

Enable and revert LIFs to home ports after a revert

During a reboot, some LIFs might have been migrated to their assigned failover ports. After you revert 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
            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.
```

Enable Snapshot copy policies after reverting

After reverting to an earlier version of ONTAP, you must enable Snapshot copy policies to

start creating Snapshot copies again.

You are reenabling the Snapshot schedules that you disabled before you reverted to an earlier version of ONTAP.

1. Enable Snapshot copy policies for all data SVMs: `volume snapshot policy modify -vserver * -enabled true``snapshot policy modify pg-rpo-hourly -enable true`
2. For each node, enable the Snapshot copy policy of the root volume by using the run-nodenodenamevol optionsroot_vol_namenosnap off command.

```
cluster1::> run -node node1 vol options vol0 nosnap off
```

Verify client access (CIFS and NFS)

For the configured protocols, test access from CIFS and NFS clients to verify that the cluster is accessible.

Verify IPv6 firewall entries

A reversion from any version of ONTAP 9 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.

1. Verify that all firewall policies are correct by comparing them to the default policies: `system services firewall policy show`

   The following example shows the default policies:

```
cluster1::*> system services firewall policy show
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 dns        allow  0.0.0.0/0
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
                 ndmp       allow  0.0.0.0/0
                 ntp        allow  0.0.0.0/0
                 rsh        allow  0.0.0.0/0
                 snmp       allow  0.0.0.0/0
                 ssh        allow  0.0.0.0/0
                 telnet     allow  0.0.0.0/0
data
                 dns        allow  0.0.0.0/0, ::/0
                 http       deny   0.0.0.0/0, ::/0
                 https      deny   0.0.0.0/0, ::/0
                 ndmp       allow  0.0.0.0/0, ::/0
                 ntp        deny   0.0.0.0/0, ::/0
                 rsh        deny   0.0.0.0/0, ::/0
.
.
.
```

2. Manually add any missing default IPv6 firewall entries by creating a new firewall policy: `system services firewall policy create`

```
cluster1::*> system services firewall policy create -policy newIPv6
-service ssh -action allow -ip-list ::/0
```

3. Apply the new policy to the LIF to allow access to a network service: `network interface modify`

```
cluster1::*> network interface modify -vserver VS1 -lif LIF1
-firewall-policy newIPv6
```

Revert password hash function to the supported encryption type

If you revert to a release prior from any version of ONTAP 9, SHA-2 account users can no longer be authenticated with their passwords. Therefore, you must have them reset their passwords to using the encryption type (MD5) that is supported by the release you revert to.

1. Prior to the revert, identify the user accounts that use the SHA-2 hash function (advanced privilege level): `security login show -vserver * -username * -application * -authentication -method password -hash-function !md5`

   You should retain the command output. You need the account information after the revert.

2. During the revert, run the advanced command security Login password-prepare-to-downgrade as prompted to reset your own password to using the MD5 hash function.

   If your password is not encrypted with MD5, the command prompts you for a new password and encrypts it with MD5, enabling your credential to be authenticated after the revert.

3. After the revert, reset SHA-2 accounts to MD5:

   a. For each SHA-2 account you identified, change the password to a temporary one: `security login password -username user_name -vserver vserver_name`

      The changed password uses the MD5 hash function.

   b. Communicate the temporary password to the affected users and have them log in through a console or SSH session to change their passwords as prompted by the system.

Considerations for whether to manually update the SP firmware

If the SP automatic update functionality is enabled (the default), downgrading or reverting to ONTAP 8.3.x does not require a manual SP firmware update. The SP firmware is automatically updated to the newest compatible version that is supported by the ONTAP version you reverted or downgraded to.

If the SP automatic update functionality is disabled (not recommended), after the ONTAP revert or downgrade process is complete, you must manually update the SP firmware to a version that is supported for the ONTAP version you reverted or downgraded to.

NetApp BIOS/ONTAP Support Matrix

NetApp Downloads: System Firmware and Diagnostics