Stage 6 Complete the upgrade

ONTAP Systems

NetApp
May 12, 2021

Table of Contents

Stage 6 Complete the upgrade

Stage 6. Complete the upgrade

During stage 6, confirm that the new nodes are set up correctly. If one of the new nodes has a unified target adapter, you must restore any port configurations and you might need to change the use of the adapter. You should also set up Storage Encryption if the new nodes are encryption-enabled.

Steps

1. Complete the upgrade for MetroCluster FC configuration
2. Ensure that the new controllers are set up correctly
3. Set up Storage Encryption on the new controller module
4. Set up NetApp Volume Encryption on the new controller module
5. Decommission the old system
6. Resume SnapMirror operations

Complete the upgrade for MetroCluster FC configuration

For a MetroCluster FC configuration, you must replace the disaster recovery/failover site nodes as soon as possible. Mismatch in controller models within a MetroCluster configuration is not supported because controller model mismatch causes disaster recovery mirroring to go offline. Use the command `-skip- metrocluster-check true` option to bypass MetroCluster checks when you are replacing nodes at a second site.

Ensure that the new controllers are set up correctly

To ensure correct setup, you must enable the HA pair. You must also verify that node3 and node4 can access each other's storage and that neither owns data LIFs belonging to other nodes on the cluster. In addition, you must ensure that node3 owns node1's aggregates and that node4 owns node2's aggregates, and that the volumes for both nodes are online.

Steps

1. After the post-checks of node2, the storage failover and cluster HA pair for the node2 cluster are enabled. When the operation is done, both nodes show as completed and the system performs some cleanup operations.

2. Verify that storage failover is enabled by entering using the following command:

   ```
   storage failover show
   ```

   The following example shows the output of the command when storage failover is enabled:

```
cluster::> storage failover show
                  Takeover
Node       Partner  Possible   State Description
--------   -----    -------    ------------------
node3      node4    true       Connected to node4
node4      node3    true       Connected to node3
```

3. Verify that node3 and node4 belong to the same cluster by using the following command and examining the output:

   cluster show

4. Verify that node3 and node4 can access each other's storage by using the following command and examining the output:

   storage failover show -fields local-missing- disks,partner-missing-disks

5. Verify that neither node3 nor node4 owns data LIFs home-owned by other nodes in the cluster by using the following command and examining the output:

   network interface show

   If neither node3 or node4 owns data LIFs home-owned by other nodes in the cluster, revert the data LIFs to their home owner by using the following command:

   network interface revert

6. Verify that node3 owns the aggregates from node1 and that node4 owns the aggregates from node2 by using the following commands:

   storage aggregate show -owner-name <node3>

   storage aggregate show -owner-name <node4>

7. Determine whether any volumes are offline by using the following commands:

   volume show -node <node3> -state offline

   volume show -node <node4> -state offline

8. If any volumes are offline, compare them with the list of offline volumes that you captured in the section Prepare the nodes for upgrade, and bring online any of the offline volumes, as required, by using the following command, once for each volume:

   volume online -vserver <vserver-name> -volume <volume_name>

9. Install new licenses for the new nodes by using the following command for each node:

   system license add - license-code <license_code,license_code,license_code…>

   The license-code parameter accepts a list of 28 upper-case alphabetic character keys. You can add one

license at a time, or you can add multiple licenses at once, separating each license key by a comma.

10. Remove all of the old licenses from the original nodes by using one of the following commands:

```
system license clean-up -unused -expired
```

```
system    license    delete    -serial-number    <node_serial_number>    -package
<licensable_package>
```

   ◦ Delete all expired licenses by using the following command:

```
system license clean-up -expired
```

   ◦ Delete all unused licenses by using the following command:

```
system license clean-up -unused
```

   ◦ Delete a specific license from a cluster by using the following commands on the nodes:

```
system license delete -serial-number <node1 serial number> -package *
```

```
system license delete -serial-number <node2 serial number> -package *
```

   The following output is displayed:

```
Warning: The following licenses will be removed:
<list of each installed package>
Do you want to continue? {y|n}: y
```

   Enter `y` to remove all of the packages.

11. Verify that the licenses are properly installed by using the following command and examining its output:

```
system license show
```

You might want to compare the output with the output that you captured in the Prepare the nodes for upgrade.

12. If NetApp Storage Encryption (NSE) was in use on the configuration and you set the `setenv bootarg.storageencryption.support` command to `true` with the `<kmip.init.maxwait>` variable `off` (in Step 27), you need to reset the variable by using the following command:

```
set    diag;    systemshell    -node    <nodename>    -command    sudo    kenv    -u    -p
kmip.init.maxwait
```

13. Configure the SPs by using the following command on both nodes:

```
system service-processor network modify -node <node_name>
```

See the System Administration Reference for information about the SPs and the ONTAP 9.8 Commands: Manual Page Reference for detailed information about the `system service- processor network modify` command.

14. Take the following actions on one of the new nodes:

   a. Enter advanced privilege level by using the following command:

   ```
   set -privilege advanced
   ```

   b. Enter the following command:

   ```
   storage   failover   modify   -node   <node_name>   -   cifs-   ndo-duration
   default|medium|low
   ```

   - Enter `medium` if the system will have workloads in which 50% to 75% of the operations will be 4 KB or smaller.

   - Enter `low` if the system will have workloads in which 75% to 100% of the operations will be 4 KB or smaller.

   c. Return to the admin level by using the following command:

   ```
   set -privilege admin
   ```

   d. Reboot the system to ensure that the changes take effect.

15. If you want to set up a switchless cluster on the new nodes, follow the instructions in **Transitioning to a two-node switchless cluster** on the NetApp Support Site.

After you finish

If Storage Encryption is enabled on node3 and node4, complete the section Set up Storage Encryption on the new controller module. Otherwise, complete the section Decommission the old system.

Set up Storage Encryption on the new controller module

If the replaced controller or the HA partner of the new controller uses Storage Encryption, you must configure the new controller module for Storage Encryption, including installing SSL certificates and setting up key management servers.

About this task

This procedure includes steps that are performed on the new controller module. You must enter the command on the correct node.

Steps

1. Verify that the key management servers are still available, their status, and their authentication key information by using the following commands:

   ```
   security key-manager show -status
   ```

   ```
   security key-manager query
   ```

2. Add the key management servers listed in the previous step to the key management server list in the new controller.

   a. Add the key management server by using the following command:

   ```
   security key-manager -add <key_management_server_ip_address>
   ```

b. Repeat the previous step for each listed key management server. You can link up to four key management servers.

c. Verify the that the key management servers were added successfully by using the following command:

```
security key-manager show
```

3. On the new controller module, run the key management setup wizard to set up and install the key management servers.

You must install the same key management servers that are installed on the existing controller module.

a. Launch the key management server setup wizard on the new node by using the following command:

```
security key-manager setup -node <new_controller_name>
```

b. Complete the steps in the wizard to configure key management servers.

4. Restore authentication keys from all linked key management servers to the new node by using the following command:

```
security key-manager restore -node <new_controller_name>
```

Set up NetApp Volume Encryption on the new controller module

If the replaced controller or the HA partner of the new controller uses NetApp Volume Encryption (NVE), you must configure the new controller module for NVE.

About this task

This procedure includes steps that are performed on the new controller module. You must enter the command on the correct node.

Steps

1. Verify that the key management servers are still available, their status, and their authentication key information:

For this ONTAP version…	Use this command…
ONTAP 9.6 and later	`security key-manager key query -node node`
ONTAP 9.5 and earlier	`security key-manager key show`

2. Add the key management servers listed in the previous step to the key management server list in the new controller:

a. Add the key management server by using the following command:

```
security key-manager -add <key_management_server_ip_address>
```

b. Repeat the previous step for each listed key management server. You can link up to four key management servers.

c. Verify the that the key management servers were added successfully by using the following command:

```
security key-manager show
```

3. On the new controller module, run the key management setup wizard to set up and install the key management servers.

You must install the same key management servers that are installed on the existing controller module.

a. Launch the key management server setup wizard on the new node by using the following command:

```
security key-manager setup -node <new_controller_name>
```

b. Complete the steps in the wizard to configure key management servers.

4. Restore authentication keys from all linked key management servers to the new node:

For…	Use this command…
External Key Manager (EKM)	`security key-manager external restore` This command needs the OKM passphrase
Onboard Key Manager (OKM)	`security key-manager onboard sync`

After you finish

Check if any volumes were taken offline because authentication keys were not available or external key management servers could not be reached. Bring those volumes back online by using the following command:

```
volume online
```

Decommission the old system

After upgrading, you can decommission the old system through the NetApp Support Site. Decommissioning the system tells NetApp that the system is no longer in operation and removes it from support databases.

Steps

1. Navigate to the NetApp Support Site and log in.

2. Select **Products > My Products** from the menu.

3. On the **View Installed Systems** page, choose which **Selection Criteria** you want to use to display information about your system.

   You can choose one of the following to locate your system:

   ◦ Serial Number (located on the back of the unit)

   ◦ Serial Numbers for My Location

4. Click **Go!**

   A table displays cluster information, including the serial numbers.

5. Locate the cluster in the table and select **Decommission this system** from the Product Tool Set drop-

down menu.

Resume SnapMirror operations

You can resume SnapMirror transfers that were quiesced before upgrade and resume the SnapMirror relationships. The updates are on schedule after the upgrade is completed.

Steps

1. Verify the SnapMirror status on the destination by using the following command:

    `snapmirror show`

2. Resume the SnapMirror relationship by using the following command:

    `snapmirror resume -destination-vserver <vserver_name>`