Replacing the controller module

You must review the prerequisites for the replacement procedure and select the correct one for your version of the ONTAP operating system.

Before you begin

- All disk shelves must be working properly.
- If your system is a FlexArray system or has a V_StorageAttach license, you must refer to the additional required steps before performing this procedure.
  - [NetApp KB Article 3015148: What are the specific steps involved in FlexArray for NetApp controller upgrades/replacements?](https://www.netapp.com)
- If your system is in an HA pair, the healthy node must be able to take over the node that is being replaced (referred to in this procedure as the impaired node).
- If you are in a MetroCluster configuration, refer to the MetroCluster Management and Disaster Recovery Guide to determine if you should use this procedure.
  - [ONTAP 9 MetroCluster Management and Disaster Recovery Guide](https://www.netapp.com)

About this task

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type; you cannot upgrade your system by just replacing the controller module.
- You cannot change any disks or disk shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired node to the replacement node so that the replacement node will boot up in the same version of ONTAP as the old controller.
- It is important that you apply the commands in these steps on the correct systems:
  - The impaired node is the node that is being replaced.
  - The replacement node is the new node that is replacing the impaired node.
  - The healthy node is the surviving node.
- You must always capture the node’s console output to a text file.
  This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

Steps

1. Shutting down the impaired controller on page 2
2. Replacing the controller module hardware on page 4
3. Restoring and verifying the system configuration on page 10
4. Completing system restoration on page 15
5. Completing the replacement process on page 21
Shutting down the impaired controller

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware configuration.

Shutting down the impaired node

To shut down the impaired node, you must determine the status of the node and, if necessary, take over the node so that the healthy node continues to serve data from the impaired node storage.

Before you begin

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy node shows false for eligibility and health, you must correct the issue before shutting down the impaired node.
  
  `ONTAP 9 System Administration Reference`

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Returning SEDs to unprotected mode" section of `ONTAP 9 NetApp Encryption Power Guide`.
  
  `ONTAP 9 NetApp Encryption Power Guide`

- If you have a SAN system, you must have checked event messages (\texttt{event log show}) for impaired node SCSI blade. Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a MetroCluster configuration, you must have confirmed that the nodes are in an enabled and normal state (\texttt{metrocluster node show}).

Steps

1. If the impaired node is part of an HA pair, disable automatic giveback from the console of the healthy node:

   \texttt{storage failover modify -node local -auto-giveback false}

2. Take the impaired node to the LOADER prompt:

   \begin{tabular}{|l|l|}
   \hline
   If the impaired node is displaying... & Then... \\ 
   \hline
   The LOADER prompt & Go to the next step. \\ 
   \hline
   Waiting for giveback... & Press Ctrl-C, and then respond \texttt{y}. \\ 
   \hline
   System prompt or password prompt & Take over or halt the impaired node: \\ & \texttt{storage failover takeover -ofnode impaired_node_name} \\
   & When the impaired node shows Waiting for giveback..., press Ctrl-C, and then respond \texttt{y}. \\
   \hline
   \end{tabular}

Shutting down a node in a two-node MetroCluster configuration running ONTAP

To shut down the impaired node, you must determine the status of the node and, if necessary, switch over the node so that the healthy node continues to serve data from the impaired node storage.

About this task

You must leave the power supplies turned on at the end of this procedure to provide power to the healthy node.
Steps

1. Check the MetroCluster status to determine whether the impaired node has automatically switched over to the healthy node:
   `metrocluster show`

2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

<table>
<thead>
<tr>
<th>If the impaired node...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has automatically switched over</td>
<td>Proceed to the next step.</td>
</tr>
<tr>
<td>Has not automatically switched over</td>
<td>Perform a planned switchover operation from the healthy node:</td>
</tr>
<tr>
<td></td>
<td><code>metrocluster switchover</code></td>
</tr>
<tr>
<td>Has not automatically switched over and planned switchover with the <code>metrocluster switchover</code> command fails</td>
<td>a. Halt the impaired node:</td>
</tr>
<tr>
<td></td>
<td><code>system node halt</code></td>
</tr>
<tr>
<td></td>
<td>b. Perform a forced switchover operation:</td>
</tr>
<tr>
<td></td>
<td><code>metrocluster switchover -forced on disaster true</code></td>
</tr>
</tbody>
</table>

3. Resynchronize the data aggregates by running the `metrocluster heal -phase aggregates` command from the surviving cluster.

   Example

   ```bash
   controller_A_1::> metrocluster heal -phase aggregates
   [Job 130] Job succeeded: Heal Aggregates is successful.
   ```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the `metrocluster operation show` command.

   Example

   ```bash
   controller_A_1::> metrocluster operation show
   Operation: heal-aggregates
   Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
   Errors: -
   ```

5. Check the state of the aggregates by using the `storage aggregate show` command.

   Example

   ```bash
   controller_A_1::> storage aggregate show
   Aggregate     Size   Available Used% State   #Vols  Nodes            RAID Status
   --------- -------- --------- ----- ------- ------ ---------------- ------------
   ... aggr_b2    227.1GB 227.1GB    0% online      0 mcc1-a2          raid_dp, mirrored,
   normal...    
   ```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.
Example

```
mcc1A::> metrocluster heal -phase root-aggregates  
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

Example

```
mcc1A::> metrocluster operation show  
    Operation: heal-root-aggregates  
    State: successful  
    End Time: 7/29/2016 20:54:42  
    Errors: -
```

8. On the impaired controller module, disconnect the power supplies.

**Replacing the controller module hardware**

To replace the controller module hardware, you must remove the impaired node, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.
Steps

1. Opening the controller module on page 5
2. Moving the boot media on page 7
3. Moving the system DIMMs on page 8
4. Installing the controller on page 10

Opening the controller module

To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.
4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

Make sure that you support the bottom of the controller module as you slide it out of the chassis.

5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.
Moving the boot media

You must locate the boot media and follow the directions to remove it from the old controller and insert it in the new controller.

Steps

1. Locate the boot media using the following illustration or the FRU map on the controller module:
2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

   **Note:** Do not twist or pull the boot media straight up, because this could damage the socket or the boot media.

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.

4. Check the boot media to make sure that it is seated squarely and completely in the socket.
   If necessary, remove the boot media and reseat it into the socket.

5. Push the boot media down to engage the locking button on the boot media housing.

### Moving the system DIMMs

To move the DIMMs, locate and move them from the old controller into the replacement controller and follow the specific sequence of steps.

**Steps**

1. If you are not already grounded, properly ground yourself.
2. Locate the DIMMs on your controller module.

3. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.

4. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.
   
   **Attention:** Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

5. Locate the slot where you are installing the DIMM.

6. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.
   
   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.
   
   **Attention:** Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

7. Insert the DIMM squarely into the slot.
   
   The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.
   
   **Attention:** Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.
8. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.

9. Repeat these steps for the remaining DIMMs.

Installing the controller

After you install the components into the controller module, you must install the controller module back into the system chassis and boot the operating system.

About this task

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

**Note:** The system might update system firmware when it boots. Do not abort this process. The procedure requires you to interrupt the boot process, which you can typically do at any time after prompted to do so. However, if the system updates the system firmware when it boots, you must wait until after the update is complete before interrupting the boot process.

Steps

1. If you are not already grounded, properly ground yourself.

2. If you have not already done so, replace the cover on the controller module.

3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

   **Note:** Do not completely insert the controller module in the chassis until instructed to do so.

4. Cable the management and console ports so that you can access the system to perform the tasks in the following sections.

5. Complete the reinstallation of the controller module:
   a. If you have not already done so, reinstall the cable management device.
   b. Firmly push the controller module into the chassis until it meets the midplane and is fully seated.

      The locking latches rise when the controller module is fully seated.

      **Attention:** Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.

      The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.

   c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.

   d. Interrupt the boot process by pressing `Ctrl-C` when you see `Press Ctrl-C for Boot Menu`.

   e. Select the option to boot to Maintenance mode from the displayed menu.

Restoring and verifying the system configuration

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.
Steps
1. Verifying and setting the HA state of the controller module on page 11
2. Running system-level diagnostics on page 12

Verifying and setting the HA state of the controller module

You must verify the HA state of the controller module and, if necessary, update the state to match your system configuration.

Steps
1. In Maintenance mode from the new controller module, verify that all components display the same HA state:

   `ha-config show`

<table>
<thead>
<tr>
<th>If your system is in...</th>
<th>The HA state for all components should be...</th>
</tr>
</thead>
<tbody>
<tr>
<td>An HA pair</td>
<td><code>ha</code></td>
</tr>
<tr>
<td>A MetroCluster FC config with four or more nodes</td>
<td><code>mcc</code></td>
</tr>
<tr>
<td>A two-node MetroCluster FC config</td>
<td><code>mcc-2n</code></td>
</tr>
</tbody>
</table>
If your system is in... | The HA state for all components should be...
---|---
A MetroCluster IP configuration | mccip
A stand-alone configuration | non-ha

2. If the displayed system state of the controller module does not match your system configuration, set the HA state for the controller module:
   
   `ha-config modify controller ha-state`

3. If the displayed system state of the chassis does not match your system configuration, set the HA state for the chassis:
   
   `ha-config modify chassis ha-state`

**Running system-level diagnostics**

You should run comprehensive or focused diagnostic tests for specific components and subsystems whenever you replace the controller.

**Before you begin**

**About this task**

All commands in the diagnostic procedures are issued from the node where the component is being replaced.

**Steps**

1. If the node to be serviced is not at the LOADER prompt, reboot the node:
   
   `halt`
   
   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly:
   
   `boot_diags`
   
   During the boot process, you can safely respond y to the prompts until the Maintenance mode prompt (*>) appears.

3. Display and note the available devices on the controller module:
   
   `sldiag device show -dev mb`

   The controller module devices and ports displayed can be any one or more of the following:

   - **bootmedia** is the system booting device.
   - **cna** is a Converged Network Adapter or interface not connected to a network or storage device.
   - **fcal** is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
   - **env** is motherboard environmental.
   - **mem** is system memory.
   - **nic** is a network interface card.
   - **nvram** is nonvolatile RAM.
   - **nvmem** is a hybrid of NVRAM and system memory.
   - **sas** is a Serial Attached SCSI device not connected to a disk shelf.
4. Run diagnostics as desired.

<table>
<thead>
<tr>
<th>If you want to run diagnostic tests on...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| Individual components                    | a. Clear the status logs:  
  `sldiag device clearstatus`  
  b. Display the available tests for the selected devices:  
  `sldiag device show -dev dev_name`  
  `dev_name` can be any one of the ports and devices identified in the preceding step.  
  c. Examine the output and, if applicable, select only the tests that you want to run:  
  `sldiag device modify -dev dev_name -selection only`  
  `-selection only` disables all other tests that you do not want to run for the device.  
  d. Run the selected tests:  
  `sldiag device run -dev dev_name`  
  After the test is complete, the following message is displayed:  
  `* > <SLDIAG:_ALL_TESTS_COMPLETED>`  
  e. Verify that no tests failed:  
  `sldiag device status -dev dev_name -long -state failed`  
  System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component. |
| Multiple components at the same time      | a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently.  
  b. List the individual tests for the device:  
  `sldiag device show -dev dev_name`  
  c. Examine the output and, if applicable, select only the tests that you want to run:  
  `sldiag device modify -dev dev_name -selection only`  
  `-selection only` disables all other tests that you do not want to run for the device.  
  d. Verify that the tests were modified:  
  `sldiag device show`  
  e. Repeat these substeps for each device that you want to run concurrently.  
  f. Run diagnostics on all of the devices:  
  `sldiag device run`  
  **Attention:** Do not add to or modify your entries after you start running diagnostics.  
  After the test is complete, the following message is displayed:  
  `* > <SLDIAG:_ALL_TESTS_COMPLETED>`  
  g. Verify that there are no hardware problems on the node:  
  `sldiag device status -long -state failed`  
  System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component. |
5. Proceed based on the result of the preceding step:

<table>
<thead>
<tr>
<th>If the system-level diagnostics tests...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Were completed without any failures</td>
<td>a. Clear the status logs:</td>
</tr>
<tr>
<td></td>
<td><code>sldiag device clearstatus</code></td>
</tr>
<tr>
<td></td>
<td>b. Verify that the log was cleared:</td>
</tr>
<tr>
<td></td>
<td><code>sldiag device status</code></td>
</tr>
<tr>
<td></td>
<td>The following default response is displayed:</td>
</tr>
<tr>
<td></td>
<td>SLDIAG: No log messages are present.</td>
</tr>
<tr>
<td></td>
<td>c. Exit Maintenance mode:</td>
</tr>
<tr>
<td></td>
<td><code>halt</code></td>
</tr>
<tr>
<td></td>
<td>The node displays the LOADER prompt.</td>
</tr>
<tr>
<td></td>
<td>d. Boot the node from the LOADER prompt:</td>
</tr>
<tr>
<td></td>
<td><code>boot_ontap</code></td>
</tr>
<tr>
<td></td>
<td>e. Return the node to normal operation:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>If your node is in...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>An HA pair</td>
<td>Perform a give back:</td>
</tr>
<tr>
<td></td>
<td><code>storage failover giveback -ofnode replacement_node_name</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you disabled automatic giveback, re-enable it with the <code>storage failover modify</code> command.</td>
</tr>
<tr>
<td>A two-node MetroCluster configuration</td>
<td>Proceed to the next step.</td>
</tr>
<tr>
<td></td>
<td>The MetroCluster healing and switchback procedures are done in the next task in the replacement process.</td>
</tr>
<tr>
<td>A stand-alone configuration</td>
<td>Proceed to the next step.</td>
</tr>
<tr>
<td></td>
<td>No action is required.</td>
</tr>
</tbody>
</table>

You have completed system-level diagnostics.
<table>
<thead>
<tr>
<th>If the system-level diagnostics tests...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resulted in some test failures</td>
<td>Determine the cause of the problem:</td>
</tr>
<tr>
<td></td>
<td>a. Exit Maintenance mode:</td>
</tr>
</tbody>
</table>
|                                        |   *halt*  
|                                        |     After you issue the command, wait until the system stops at the LOADER prompt. |
|                                        | b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis: |
|                                        |   • If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module. |
|                                        |   • If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources. |
|                                        | c. Verify that you have observed all the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system. |
|                                        | d. Boot the controller module you are servicing, interrupting the boot by pressing *Ctrl-C* when prompted to get to the Boot menu: |
|                                        |   • If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis.  
|                                        |     The controller module boots up when fully seated. |
|                                        |   • If you have one controller module in the chassis, connect the power supplies, and then turn them on. |
|                                        | e. Select Boot to maintenance mode from the menu. |
|                                        | f. Exit Maintenance mode by entering the following command: |
|                                        |   *halt*  
|                                        |     After you issue the command, wait until the system stops at the LOADER prompt. |
|                                        | g. Rerun the system-level diagnostic test. |

### Completing system restoration

To complete the replacement procedure and restore your system to full operation, you must recable the storage, restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller.
Recabling the system

After running diagnostics, you must recable the controller module's storage and network connections.

**Steps**

1. Recable the system.
2. Verify that the cabling is correct by using Config Advisor.
   a. Download and install Config Advisor from the NetApp Support Site.
      
      `mysupport.netapp.com`
   b. Enter the information for the target system, and then click **Collect Data**.
   c. Click the **Cabling** tab, and then examine the output.
      Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.
Installing licenses for the replacement node in ONTAP

You must install new licenses for the replacement node if the impaired node was using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the replacement node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the replacement node as soon as possible.

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

**Note:** If the node is in a MetroCluster configuration and all nodes at a site have been replaced (a single node in the case of a two-node MetroCluster configuration), license keys must be installed on the replacement node or nodes prior to switchback.

**Note:** If the node is in a MetroCluster configuration and all nodes at a site have been replaced, license keys must be installed on the replacement node or nodes prior to switchback.

Steps

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

   **NetApp Support**

   **Note:** The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

2. Install each license key:

   `system license add -license-code license-key, license-key...`

3. Remove the old licenses, if desired:

   a. Check for unused licenses:

      `license clean-up -unused -simulate`

   b. If the list looks correct, remove the unused licenses:

      `license clean-up -unused`

Restoring Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in the *NetApp Encryption Power Guide*.

   **ONTAP 9 NetApp Encryption Power Guide**

   Use one of the following procedures, depending on whether you are using onboard or external key management:

   - “Restoring onboard key management encryption keys”
Verifying LIFs and registering the serial number

Before returning the replacement node to service, you should verify that the LIFs are on their home ports, and register the serial number of the replacement node if AutoSupport is enabled, and reset automatic giveback.

**Steps**

1. Verify that the logical interfaces are reporting to their home server and ports:
   ```
   network interface show -is-home false
   ```
   If any LIFs are listed as `false`, revert them to their home ports:
   ```
   network interface revert *
   ```

2. Register the system serial number with NetApp Support.
   
<table>
<thead>
<tr>
<th>If...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoSupport is enabled</td>
<td>Send an AutoSupport message to register the serial number.</td>
</tr>
<tr>
<td>AutoSupport is not enabled</td>
<td>Call NetApp Support to register the serial number.</td>
</tr>
</tbody>
</table>

3. If automatic giveback was disabled, reenable it:
   ```
   storage failover modify -node local -auto-giveback true
   ```

Healing and switching back aggregates in a two-node MetroCluster configuration

After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster healing and switchback operations. These operations return the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

**About this task**

This task only applies to two-node MetroCluster configurations.

**Steps**

1. Resynchronize the aggregates by using the `metrocluster heal -phase aggregates` command from the surviving cluster.

   **Example**
   ```
   controller_A_1::> metrocluster heal -phase aggregates
   [Job 130] Job succeeded: Heal Aggregates is successful.
   ```
   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

2. Verify that the operation was completed successfully by using the `metrocluster operation show` command.
Example

ccontroller_A_1::> metrocluster operation show
  Operation: heal-aggregates
  State: successful
  Start Time: 7/25/2014 18:45:55
  End Time: 7/25/2014 18:45:56
  Errors: -

3. Check the state of the aggregates by using the `storage aggregate show` command.

Example

ccontroller_A_1::> storage aggregate show
  Aggregate     Size Available Used% State   #Vols  Nodes            RAID Status
  --------- -------- --------- ----- ------- ------ ---------------- ------------
  ...        ...        ...        ...    ...    ...    ...                        ...
  aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2          raid_dp, mirrored, normal...

4. Switch back the mirrored aggregates by using the `metrocluster heal -phase root-aggregates` command.

Example

ccontroller_A_1::> metrocluster heal -phase root-aggregates
  [Job 137] Job succeeded: Heal Root Aggregates is successful

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

5. Verify that the heal operation was completed successfully by using the `metrocluster operation show` command on the healthy cluster:

Example

ccontroller_A_1::> metrocluster operation show
  Operation: heal-root-aggregates
  State: successful
  End Time: 7/29/2014 20:54:42
  Errors: -

6. Verify that all nodes are in the enabled state:

   `metrocluster node show`

Example

ccontroller_A_1::> metrocluster node show
  DR Group Cluster Node           State          Mirroring Mode
  ----- ------- -------------- -------------- --------- -------------------
  1     --controller_A_1 configured enabled heal roots completed
  2     --controller_B_1 configured enabled waiting for switchback recovery
  2 entries were displayed.

7. Verify that resynchronization is complete on all SVMs:

   `metrocluster vserver show`

Completing system restoration
8. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully:
   `metrocluster check lif show`

9. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.

10. Verify that the switchback operation has completed:
    `metrocluster show`

**Example**

The switchback operation is still running when a cluster is in the waiting-for-switchback state:

```
cluster_B::> metrocluster show
Cluster  | Configuration State | Mode
---------|---------------------|------
Local:   | cluster_B configured| switchover
Remote:  | cluster_A configured| waiting-for-switchback
```

The switchback operation is complete when the clusters are in the normal state:

```
cluster_B::> metrocluster show
Cluster  | Configuration State | Mode
---------|---------------------|------
Local:   | cluster_B configured| normal
Remote:  | cluster_A configured| normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

11. Reestablish any SnapMirror or SnapVault configurations.

### Setting and verifying system time after replacing the controller

You should check the time and date on the replacement controller module against the healthy controller module in an HA pair, or against a reliable time server in a stand-alone configuration. If the time and date do not match, you must reset them on the replacement controller module to prevent possible outages on clients due to time differences.

**About this task**

It is important that you apply the commands in the steps on the correct systems:

- The **replacement node** is the new node that replaced the impaired node as part of this procedure.
- The **healthy node** is the HA partner of the replacement node

**Steps**

1. In `admin` privilege on the replacement node, check the system time on the nodes:
   `cluster date show`
   The date and time are displayed for all nodes in the cluster.

2. If necessary, set the time on the replacement node to match the healthy node:
   `cluster date modify -dateandtime "target_date_and_time"`

3. Check the date and time from the replacement node:
   `cluster date show`

4. Exit `admin` privilege.
Completing the replacement process

After you replace the part, you can return the failed part to NetApp, as described in the RMA instructions shipped with the kit. Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Copyright information

Copyright © 2018 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, tapping, 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferable, non-sublicensable, 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).

Trademark information

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

• NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277