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 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

About this task

- This procedure includes steps for automatically or manually reassigning disks to the replacement node, depending on your system's configuration.
  You should perform the disk reassignment as directed in the procedure.
- 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.
- Any PCIe cards moved from the old controller module to the new controller module or added from existing customer site inventory must be supported by the replacement controller module.

NetApp Hardware Universe

- 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 12
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 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 (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 (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:

   ```bash
   storage failover modify -node local -auto-giveback false
   ```

2. Take the impaired node to the LOADER prompt:

<table>
<thead>
<tr>
<th>If the impaired node is displaying...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>The LOADER prompt</td>
<td>Go to the next step.</td>
</tr>
<tr>
<td>Waiting for giveback...</td>
<td>Press Ctrl-C, and then respond y when prompted.</td>
</tr>
</tbody>
</table>
If the impaired node is displaying... Then...

System prompt or password prompt Take over or halt the impaired node:
  • For an HA pair, take over the impaired node from the healthy node:
    `storage failover takeover -ofnode impaired_node_name`
    When the impaired node shows Waiting for giveback..., press Ctrl-C, and then respond `y`.
  • For a stand-alone system:
    `system node halt impaired_node_name`

3. If the system has only one controller module in the chassis, turn off the power supplies, and then unplug the impaired node’s power cords from the power source.

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: <code>metrocluster switchover</code></td>
</tr>
</tbody>
</table>
| Has not automatically switched over and planned switchover with the `metrocluster switchover` command fails | a. Halt the impaired node: `system node halt`  
  b. Perform a forced switchover operation: `metrocluster switchover -forced on disaster true` |

3. Resynchronize the data aggregates by running 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.

4. Verify that the operation has been completed by using the `metrocluster operation show` command.
5. Check the state of the aggregates by using the `storage aggregate show` command.

Example

```
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 device** on page 6
3. **Moving the NVMEM battery** on page 7
4. **Moving the DIMMs** on page 9
5. **Moving a PCIe card** on page 10
6. **Installing the controller** on page 11

**Opening the controller module**

To replace the controller module, you must first remove the old controller module from the chassis.

**Steps**

1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.
Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

3. Remove and set aside the cable management devices from the left and right sides of the controller module.

   ![Diagram](image)

4. If you left the SFP modules in the system after removing the cables, move them to the new controller module.

5. Loosen the thumbscrew on the cam handle on the controller module.

   ![Diagram](image)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Thumbscrew</td>
</tr>
<tr>
<td>2</td>
<td>Cam handle</td>
</tr>
</tbody>
</table>

6. Pull the cam handle downward and begin to 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.

**Moving the boot device**

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 NVMEM battery**

To move the NVMEM battery from the old controller module to the new controller module, you must perform a specific sequence of steps.

**Steps**

1. Check the NVMEM LED:
   
   • If your system is in an HA configuration, go to the next step.
   
   • If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.
Attention: The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

- If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
- If the LED is on and power is on, unwritten data is stored on NVMEM. This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Open the CPU air duct and locate the NVMEM battery.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Battery lock tab</td>
</tr>
<tr>
<td>2</td>
<td>NVMEM battery pack</td>
</tr>
</tbody>
</table>
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.

4. Remove the battery from the controller module and set it aside.

Moving the 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. Locate the DIMMs on your controller module.

2. 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.

3. 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.

The number and placement of system DIMMs depends on the model of your system.

The following illustration shows the location of system DIMMs:
4. Locate the slot where you are installing the DIMM.

5. 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.

6. Repeat these steps for the remaining DIMMs.

7. Move the NVMEM battery to the replacement controller module.

8. Align the tab or tabs on the battery holder with the notches in the controller module side, and then gently push down on the battery housing until the battery housing clicks into place.

**Moving a PCIe card**

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

**Before you begin**

You must have the new controller module ready so that you can move the PCIe cards directly from the old controller module to the corresponding slots in the new one.

**Steps**

1. Loosen the thumbscrew on the controller module side panel.

2. Swing the side panel off the controller module.
3. Remove the PCIe card from the old controller module and set it aside. Make sure that you keep track of which slot the PCIe card was in.

4. Repeat the preceding step for the remaining PCIe cards in the old controller module.

5. Open the new controller module side panel, if necessary, slide off the PCIe card filler plate, as needed, and carefully install the PCIe card.
   
   Be sure that you properly align the card in the slot and exert even pressure on the card when seating it in the socket. The card must be fully and evenly seated in the slot.

6. Repeat the preceding step for the remaining PCIe cards that you set aside.

7. Close the side panel and tighten the thumbscrew.

**Installing the controller**

After you install the components from the old controller module into the new controller module, you must install the new controller module 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, close the CPU air duct.

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:
<table>
<thead>
<tr>
<th>If your system is in...</th>
<th>Then perform these steps...</th>
</tr>
</thead>
</table>
| An HA pair             | The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.  
  
  a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module.  
    **Attention:** Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.  
    The controller begins to boot as soon as it is seated in the chassis.  
  
  b. If you have not already done so, reinstall the cable management device.  
  
  c. Bind the cables to the cable management device with the hook and loop strap.  
  
  d. When you see the message **Press Ctrl-C for Boot Menu**, press **Ctrl-C** to interrupt the boot process.  
    **Note:** If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press **Ctrl-C** when prompted, and then boot to Maintenance mode.  
  
  e. Select the option to boot to Maintenance mode from the displayed menu. |
| A stand-alone configuration | With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module.  
    **Attention:** Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.  
  
  b. If you have not already done so, reinstall the cable management device.  
  
  c. Bind the cables to the cable management device with the hook and loop strap.  
  
  d. Reconnect the power cables to the power supplies and to the power sources, turn on the power to start the boot process, and then press **Ctrl-C** after you see the **Press Ctrl-C for Boot Menu** message.  
    **Note:** If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press **Ctrl-C** when prompted, and then boot to Maintenance mode.  
  
  e. From the boot menu, select the option for Maintenance mode. |

**Important:** During the boot process, you might see the following prompts:  
- A prompt warning of a system ID mismatch and asking to override the system ID.  
- A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy node remains down.  

You can safely respond `y` to these prompts.

**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 13
2. Running system-level diagnostics on page 14

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>ha</td>
</tr>
<tr>
<td>A MetroCluster FC config with four or more nodes</td>
<td>mcc</td>
</tr>
<tr>
<td>A two-node MetroCluster FC configuration</td>
<td>mcc-2n</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>
<tbody>
<tr>
<td>Individual components</td>
<td></td>
</tr>
<tr>
<td>a. Clear the status logs:</td>
<td></td>
</tr>
<tr>
<td><code>sldiag device clearstatus</code></td>
<td></td>
</tr>
<tr>
<td>b. Display the available tests for the selected devices:</td>
<td></td>
</tr>
<tr>
<td><code>sldiag device show -dev dev_name</code></td>
<td></td>
</tr>
<tr>
<td><code>dev_name</code> can be any one of the ports and devices identified in the preceding step.</td>
<td></td>
</tr>
<tr>
<td>c. Examine the output and, if applicable, select only the tests that you want to run:</td>
<td></td>
</tr>
<tr>
<td><code>sldiag device modify -dev dev_name -selection only</code></td>
<td></td>
</tr>
<tr>
<td><code>-selection only</code> disables all other tests that you do not want to run for the device.</td>
<td></td>
</tr>
<tr>
<td>d. Run the selected tests:</td>
<td></td>
</tr>
<tr>
<td><code>sldiag device run -dev dev_name</code></td>
<td></td>
</tr>
<tr>
<td>After the test is complete, the following message is displayed:</td>
<td></td>
</tr>
<tr>
<td><code>* &gt; &lt;SLDIAG:_ALL_TESTS_COMPLETED&gt;</code></td>
<td></td>
</tr>
<tr>
<td>e. Verify that no tests failed:</td>
<td></td>
</tr>
<tr>
<td><code>sldiag device status -dev dev_name -long -state failed</code></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

| 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 system displays the LOADER prompt.</td>
</tr>
<tr>
<td></td>
<td>You have completed system-level diagnostics.</td>
</tr>
<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>
<tr>
<td></td>
<td><code>halt</code></td>
</tr>
<tr>
<td></td>
<td>b. Perform a clean shutdown, and then disconnect the power supplies.</td>
</tr>
<tr>
<td></td>
<td>c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.</td>
</tr>
<tr>
<td></td>
<td>d. Reconnect the power supplies, and then power on the storage system.</td>
</tr>
<tr>
<td></td>
<td>e. Rerun the system-level diagnostics test.</td>
</tr>
</tbody>
</table>

Completing system restoration

To complete the replacement procedure and restore your system to full operation, you must recable the storage, confirm disk reassignment, 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.
   - If you removed the media converters (SFPs), remember to reinstall them if you are using fiber optic cables.
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.

**Reassigning disks**

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. In a stand-alone system, you must manually reassign the ID to the disks.

**About this task**

You must use the correct procedure for your configuration:

<table>
<thead>
<tr>
<th>Controller redundancy</th>
<th>Then use this procedure...</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA pair</td>
<td><strong>Verifying the system ID change on an HA system</strong> on page 18</td>
</tr>
<tr>
<td>Stand-alone</td>
<td><strong>Manually reassigning the system ID on a stand-alone system in ONTAP</strong> on page 20</td>
</tr>
<tr>
<td>Two-node MetroCluster configuration</td>
<td><strong>Manually reassigning the system ID on systems in a two-node MetroCluster configuration</strong> on page 21</td>
</tr>
</tbody>
</table>

**Verifying the system ID change on an HA system**

You must confirm the system ID change when you boot the replacement node and then verify that the change was implemented.

**About this task**

This procedure applies only to systems running ONTAP in an HA pair.

**Steps**

1. If the replacement node is in Maintenance mode (showing the * > prompt, exit Maintenance mode and go to the LOADER prompt:
   ```
   halt
   ```

2. From the LOADER prompt on the replacement node, boot the node, entering `y` if you are prompted to override the system ID due to a system ID mismatch:
   ```
   boot_ontap
   ```

3. Wait until the `Waiting for giveback...` message is displayed on the replacement node console and then, from the healthy node, verify that the new partner system ID has been automatically assigned:
   ```
   storage failover show
   ```

**Example**

In the command output, you should see a message that the system ID has changed on the impaired node, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.

```
node1> storage failover show

<table>
<thead>
<tr>
<th>Node</th>
<th>Partner</th>
<th>Takeover</th>
<th>State Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1</td>
<td>node2</td>
<td>false</td>
<td>System ID changed on partner (Old: 151759755, New: 151759706), Incomplete takeover</td>
</tr>
<tr>
<td>takeover</td>
<td>node2</td>
<td>false</td>
<td>Waiting for giveback (HA mailboxes)</td>
</tr>
</tbody>
</table>
```

4. From the healthy node, verify that any coredumps are saved:
a. Change to the advanced privilege level:

\texttt{set -privilege advanced}

You can respond \texttt{y} when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

b. Save any coredumps:

\texttt{system node run -node local-node-name partner savecore}

c. Wait for savecore command to complete before issuing the giveback.

You can enter the following command to monitor the progress of the savecore command:

\texttt{system node run -node local-node-name partner savecore -s}

d. Return to the admin privilege level:

\texttt{set -privilege admin}

5. Give back the node:

a. From the healthy node, give back the replaced node's storage:

\texttt{storage failover giveback -ofnode replacement_node_name}

The replacement node takes back its storage and completes booting.

If you are prompted to override the system ID due to a system ID mismatch, you should enter \texttt{y}.

\textbf{Note:} If the giveback is vetoed, you can consider overriding the vetoes.

\textit{Find the High-Availability Configuration Guide for your version of ONTAP 9}

b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: \texttt{storage failover show}

The output from the \texttt{storage failover show} command should not include the System ID changed on partner message.

6. If the system is in a MetroCluster configuration, monitor the status of the node:

\texttt{metrocluster node show}

The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each node will show a configured state, with DR Mirroring enabled and a mode of normal. The \texttt{metrocluster node show -fields node-systemid} command output displays the old system ID until the MetroCluster configuration returns to a normal state.

7. Verify that the disks were assigned correctly:

\texttt{storage disk show -ownership}

\textbf{Example}

The disks belonging to the replacement node should show the new system ID. In the following example, the disks owned by node1 now show the new system ID, 1873775277:

```
node1> storage disk show -ownership

<table>
<thead>
<tr>
<th>Disk</th>
<th>Aggregate</th>
<th>Home</th>
<th>Owner</th>
<th>DR Home</th>
<th>Home ID</th>
<th>Owner ID</th>
<th>DR Home ID</th>
<th>Reserver</th>
<th>Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>aggr0_1</td>
<td>node1</td>
<td>node1</td>
<td>-</td>
<td>1873775277</td>
<td>1873775277</td>
<td>1873775277</td>
<td>-</td>
<td>Pool0</td>
</tr>
<tr>
<td>1.0.1</td>
<td>aggr0_1</td>
<td>node1</td>
<td>node1</td>
<td>1873775277</td>
<td>1873775277</td>
<td>1873775277</td>
<td>1873775277</td>
<td>Pool0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Completing system restoration 19
8. If the node is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a node on the disaster site.

This is required if both of the following are true:

- The MetroCluster configuration is in a switchover state.
- The replacement node is the current owner of the disks on the disaster site.

9. If your system is in a MetroCluster configuration, verify that each node is configured:

   `metrocluster node show -fields configuration-state`

Example

```
node1_siteA::> metrocluster node show -fields configuration-state

+--------+-----------------------+-------------------+
<table>
<thead>
<tr>
<th>dr-group-id</th>
<th>cluster node</th>
<th>configuration-state</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 node1_siteA</td>
<td>node1mcc-001</td>
<td>configured</td>
</tr>
<tr>
<td>1 node1_siteA</td>
<td>node1mcc-002</td>
<td>configured</td>
</tr>
<tr>
<td>1 node1_siteB</td>
<td>node1mcc-003</td>
<td>configured</td>
</tr>
<tr>
<td>1 node1_siteB</td>
<td>node1mcc-004</td>
<td>configured</td>
</tr>
</tbody>
</table>
+--------+-----------------------+-------------------+
4 entries were displayed.
```

10. Verify that the expected volumes are present for each node:

   `vol show -node node-name`

11. If you disabled automatic takeover on reboot, enable it from the healthy node:

   `storage failover modify -node replacement-node-name -onreboot true`

Manually reassigning the system ID on a stand-alone system in ONTAP

In a stand-alone system, you must manually reassign disks to the new controller's system ID before you return the system to normal operating condition.

About this task

This procedure applies only to systems that are in a stand-alone configuration.

Steps

1. If you have not already done so, reboot the replacement node, interrupt the boot process by pressing Ctrl-C, and then select the option to boot to Maintenance mode from the displayed menu.

   You must enter `Y` when prompted to override the system ID due to a system ID mismatch.

2. View the system IDs:

   `disk show -a`

   You should make a note of the old system ID, which is displayed as part of the disk owner column.

Example

The following example shows the old system ID of 118073209:
3. Boot the node:

```
boot_ontap
```

### Manually reassigning the system ID on systems in a two-node MetroCluster configuration

In a two-node MetroCluster configuration running ONTAP, you must manually reassign disks to the new controller’s system ID before you return the system to normal operating condition.

#### About this task

This procedure applies only to systems in a two-node MetroCluster configuration running ONTAP.

You must be sure to issue the commands in this procedure on the correct node:

- The *impaired node* is the node on which you are performing maintenance.
- The *replacement node* is the new node that replaced the impaired node as part of this procedure.
- The *healthy node* is the DR partner of the impaired node.

#### Steps

1. If you have not already done so, reboot the replacement node, interrupt the boot process by entering `Ctrl-C`, and then select the option to boot to Maintenance mode from the displayed menu.
   
   You must enter `Y` when prompted to override the system ID due to a system ID mismatch.

2. View the old system IDs from the healthy node:

   ```
   metrocluster node show -fields node-systemid,dr-partner-systemid
   ```

   **Example**

   In this example, the Node_B_1 is the old node, with the old system ID of 118073209:

<table>
<thead>
<tr>
<th>dr-group-id</th>
<th>cluster</th>
<th>node</th>
<th>node-systemid</th>
<th>dr-partner-systemid</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cluster_A</td>
<td>Node_A_1</td>
<td>536872914</td>
<td>118073209</td>
</tr>
<tr>
<td>1</td>
<td>Cluster_B</td>
<td>Node_B_1</td>
<td>118073209</td>
<td>536872914</td>
</tr>
<tr>
<td>2 entries were displayed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. View the new system ID at the Maintenance mode prompt on the impaired node:

```
* disk show -a
Local System ID: 118065481

<table>
<thead>
<tr>
<th>DISK</th>
<th>OWNER</th>
<th>POOL</th>
<th>SERIAL NUMBER</th>
<th>HOME</th>
</tr>
</thead>
<tbody>
<tr>
<td>disk_name</td>
<td>system-1</td>
<td>Pool0</td>
<td>J8XJE9LC</td>
<td>system-1</td>
</tr>
<tr>
<td>disk_name</td>
<td>system-1</td>
<td>Pool0</td>
<td>J8Y478RC</td>
<td>system-1</td>
</tr>
</tbody>
</table>
```

```
Example

In this example, the new system ID is 118065481:
```

4. Reassign disk ownership (for FAS systems) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the `disk show` command:

   `disk reassign -s old system ID`

   In the case of the preceding example, the command is: `disk reassign -s 118073209`

   You can respond Y when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly:

   `disk show -a`

   **Example**

   Verifying that the disks belonging to the replacement node show the new system ID for the replacement node. In the following example, the disks owned by system-1 now show the new system ID, 118065481:

   ```
   *> disk show -a
   Local System ID: 118065481
   DISK     OWNER                 POOL   SERIAL NUMBER  HOME
   -------    -------------         -----  -------------  -------------
disk_name  system-1  (118065481) Pool0  J8Y0TDZC       system-1  (118065481)
disk_name  system-1  (118065481) Pool0  J8Y09DXC       system-1  (118065481)
```

6. From the healthy node, verify that any coredumps are saved:

   a. Change to the advanced privilege level:

      `set -privilege advanced`

      You can respond Y when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Verify that the coredumps are saved:

      `system node run -node local-node-name partner savecore`

      If the command output indicates that savecore is in progress, wait for savecore to complete before issuing the giveback. You can monitor the progress of the savecore using the `system node run -node local-node-name partner savecore -s` command.</info>.

   c. Return to the admin privilege level:

      `set -privilege admin`

7. If the replacement node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt:

   `halt`

8. Boot the replacement node:

   `boot_ontap`

9. After the replacement node has fully booted, perform a switchback:

   `metrocluster switchback`

10. Verify the MetroCluster configuration:
**Example**

```
node1_siteA::> metrocluster node show -fields configuration-state
```

<table>
<thead>
<tr>
<th>dr-group-id</th>
<th>cluster node</th>
<th>configuration-state</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 node1_siteA</td>
<td>node1mcc-001</td>
<td>configured</td>
</tr>
<tr>
<td>1 node1_siteA</td>
<td>node1mcc-002</td>
<td>configured</td>
</tr>
<tr>
<td>1 node1_siteB</td>
<td>node1mcc-003</td>
<td>configured</td>
</tr>
<tr>
<td>1 node1_siteB</td>
<td>node1mcc-004</td>
<td>configured</td>
</tr>
</tbody>
</table>

4 entries were displayed.

11. Verify the operation of the MetroCluster configuration in Data ONTAP:

   a. Check for any health alerts on both clusters:
      
      ```
system health alert show
      ```
   
   b. Confirm that the MetroCluster is configured and in normal mode:
      
      ```
metrocluster show
      ```
   
   c. Perform a MetroCluster check:
      
      ```
metrocluster check run
      ```
   
   d. Display the results of the MetroCluster check:
      
      ```
metrocluster check show
      ```
   

      After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

12. Simulate a switchover operation:

   a. From any node's prompt, change to the advanced privilege level:
      
      ```
set -privilege advanced
      ```

      You need to respond with y when prompted to continue into advanced mode and see the advanced mode prompt (*>).

   b. Perform the switchback operation with the -simulate parameter:
      
      ```
metrocluster switchover -simulate
      ```
   
   c. Return to the admin privilege level:
      
      ```
set -privilege admin
      ```

**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:

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

3. Remove the old licenses, if desired:
   a. Check for unused licenses:

      ```bash
      license clean-up -unused -simulate
      ```
   b. If the list looks correct, remove the unused licenses:

      ```bash
      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”
   - “Restoring external 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:

   ```bash
   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**
   ```
   controller_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**
   ```
   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...    
   ```
4. Switch back the mirrored 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.

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

Example

```
mcc1A::> 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

```
cluster_B::> metrocluster node show
DR Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- --------- --------------------
1     cluster_A
      controller_A_1 configured     enabled   heal roots completed
cluster_B
      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
```

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.
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, taping, 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-transferrable, 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