Replacing the NVRAM10 module and/or DIMMs

The NVRAM module consists of the NVRAM10 and DIMMs and up to two NVMe SSD Flash Cache modules (FlashCache or caching modules) per NVRAM module. You can replace a failed NVRAM module or the DIMMs inside the NVRAM module. To replace a failed NVRAM module, you must remove it from the chassis, remove the FlashCache module or modules from the NVRAM module, move the DIMMs to the replacement module, reinstall the FlashCache module or modules, and install the replacement NVRAM module into the chassis. Because the system ID is derived from the NVRAM module, if replacing the module, disks belonging to the system are reassigned to the new system ID.

Before you begin

- All disk shelves must be working properly.
- If your system is in an HA pair, the partner node must be able to take over the node associated with the NVRAM module that is being replaced.

About this task

- This procedure uses the following terminology:
  - The impaired node is the node on which you are performing maintenance.
  - The healthy node is the HA partner of the impaired node.
- This procedure includes steps for automatically or manually reassigning disks to the controller module associated with the new NVRAM module. You must reassign the disks when directed to in the procedure. Completing the disk reassignment before giveback can cause issues.
- You must replace the failed component with a replacement FRU component you received from your provider.
- You cannot change any disks or disk shelves as part of this procedure.

Steps

1. Pre-replacement tasks for systems that use Storage Encryption on page 2
2. Shutting down the impaired node on page 2
3. Replacing the NVRAM module on page 3
4. Replacing a NVRAM DIMM on page 5
5. Rebooting the controller after FRU replacement on page 7
6. Reassigning disks on page 7
7. Restoring Storage and Volume Encryption functionality on page 12
8. Completing the replacement process on page 12
Pre-replacement tasks for systems that use Storage Encryption

If you are replacing a controller module in a system with Storage Encryption enabled, you must first reset the authentication keys of the disks to their MSID (the default security ID set by the manufacturer). This is a temporary necessity to avoid losing access to the data.

About this task

After resetting the authentication keys to the MSID, the data on the disks is no longer protected by secret authentication keys. You must ensure the physical safety of the disks during the replacement or upgrade process.

Steps

1. Set the privilege level to advanced:
   ```bash
   set -privilege advanced
   ```
2. Reset the MSID using the instructions in the "Returning SEDs to unprotected mode" section.
   *ONTAP 9 NetApp Encryption Power Guide*
3. Exit advanced mode:
   ```bash
   set -privilege admin
   ```

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.

Steps

1. If you have a cluster with more than two nodes, check the health and Epsilon from advanced mode:
   ```bash
   cluster show -epsilon *
   ```
   If the cluster is not in quorum or a node that is not the impaired node shows `false` for eligibility and health, correct the issue before proceeding to the next step.
   If Epsilon resides in the impaired node:
   a. Remove Epsilon from the impaired node:
      ```bash
      cluster modify -node impaired_node -epsilon false
      ```
   b. Assign Epsilon to a healthy node in the cluster:
      ```bash
      cluster modify -node healthy_node -epsilon true
      ```
2. 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
   ```
3. 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.</td>
</tr>
</tbody>
</table>
| System prompt or password prompt | Take over or halt the impaired node:  
                          
                          storage failover takeover -ofnode impaired_node_name  
                          When the impaired node shows Waiting for giveback..., press Ctrl-C, and then respond y. |

**Replacing the NVRAM module**

To replace the NVRAM module, locate it in slot 6 in the chassis and follow the specific sequence of steps.

**Steps**

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

2. Move the FlashCache module from the old NVRAM module to the new NVRAM module:

   a. Press the orange button on the front of the FlashCache module.

   **Note:** The release button on empty FlashCache modules is gray.
b. Swing the cam handle out until the module begins to slide out of the old NVRAM module.

c. Grasp the module cam handle and slide it out of the NVRAM module and insert it into the front of the new NVRAM module.

d. Gently push the FlashCache module all the way into the NVRAM module and then swing the cam closed until it locks the module in place.

3. Remove the target NVRAM module from the chassis:
   a. Depress the lettered and numbered cam button.
      The cam button moves away from the chassis.
   b. Rotate the cam latch down until it is in a horizontal position.
      The NVRAM module disengages from the chassis and moves a few inches out.
   c. Remove the NVRAM module from the chassis by pulling on the pull tabs on the sides of the module face.

4. Set the NVRAM module on a stable surface and remove the cover from the NVRAM module by pushing down on the blue locking button on the cover, and then, while holding the blue button down, slide the lid off the module.
5. Remove the DIMMs, one at a time, from the old NVRAM module and install them in the replacement NVRAM module.
6. Close the cover on the module.
7. Install the replacement NVRAM module into the chassis:
   a. Align the module with the edges of the chassis opening in slot 6.
   b. Gently slide the module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

**Replacing a NVRAM DIMM**

To replace NVRAM DIMMs in the NVRAM module, you must remove the NVRAM module, open the module, and then replace the target DIMM.

**Steps**

1. If you are not already grounded, properly ground yourself.
2. Remove the target NVRAM module from the chassis:
   a. Depress the lettered and numbered cam button.
      The cam button moves away from the chassis.
   b. Rotate the cam latch down until it is in a horizontal position.
      The NVRAM module disengages from the chassis and moves a few inches out.
   c. Remove the NVRAM module from the chassis by pulling on the pull tabs on the sides of the module face.
1. Lettered and numbered I/O cam latch

2. I/O latch completely unlocked

3. Set the NVRAM module on a stable surface and remove the cover from the NVRAM module by pushing down on the blue locking button on the cover, and then, while holding the blue button down, slide the lid off the module.
1. Cover locking button
2. DIMM and DIMM ejector tabs

4. Locate the DIMM to be replaced inside the NVRAM module and remove it by pressing down on the DIMM locking tabs, and then lift the DIMM out of the socket. Each DIMM has an LED next to it that flashes when the DIMM has failed.

5. Install the replacement DIMM by aligning the DIMM with the socket and gently pushing the DIMM into the socket until the locking tabs lock in place.

6. Close the cover on the module.

7. Install the replacement NVRAM module into the chassis:
   a. Align the module with the edges of the chassis opening in slot 6.
   b. Gently slide the module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

**Rebooting the controller after FRU replacement**

After you replace the FRU, you must reboot the controller module.

**Step**

1. Boot to Maintenance mode:
   a. From the LOADER prompt, enter **bye**, and then boot the node to Maintenance mode interrupting the boot process by pressing **Ctrl-C** when you see **Press Ctrl-C for Boot Menu**.
   b. Select the option to boot to Maintenance mode from the displayed menu.

   **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.

**Reassigning disks**

Depending on your configuration, you must either verify the reassignment of disks to the new controller module or manually reassign the 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:
Controller module redundancy | Then use this procedure...
---|---
HA pair | Verifying the system ID change on an HA system on page 8
Two-node MetroCluster configuration | Manually reassigning the system ID on systems in a two-node MetroCluster configuration on page 10

**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.

**Example**

<table>
<thead>
<tr>
<th>Node</th>
<th>Partner</th>
<th>Possible</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), In takeover</td>
</tr>
</tbody>
</table>

4. 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. Save any coredumps:
      ```
      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:
      ```
      system node run -node local-node-name partner savecore -s
      ```
   d. Return to the admin privilege level:
      ```
      set -privilege admin
      ```
5. Give back the node:
a. From the healthy node, give back the replaced node's storage:

```bash
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 `y`.

**Note:** If the giveback is vetoed, you can consider overriding the vetoes.

*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: `storage failover show`

The output from the `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:

```bash
metrocluster node show
```

The MetroCluster configuration takes a few minutes after the replacement to return to a normal state. The `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

7. 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.

*ONTAP 9 MetroCluster Management and Disaster Recovery Guide*

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

```bash
metrocluster node show -fields configuration-state
```

*ONTAP 9 MetroCluster Management and Disaster Recovery Guide*

**Example**

```
nodel_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</td>
<td>nodelmcc-001</td>
<td>configured</td>
</tr>
<tr>
<td>1</td>
<td>nodelmcc-002</td>
<td>configured</td>
</tr>
<tr>
<td>1</td>
<td>nodelmcc-003</td>
<td>configured</td>
</tr>
<tr>
<td>1</td>
<td>nodelmcc-004</td>
<td>configured</td>
</tr>
</tbody>
</table>

4 entries were displayed.
```

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

```bash
vol show -node node-name
```

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

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

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

FAS9000 systems: Replacing the NVRAM10 module and/or DIMMs
Example
Verify 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

<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>J8Y0TDZC</td>
<td>system-1 (118065481)</td>
</tr>
<tr>
<td>disk_name</td>
<td>system-1</td>
<td>Pool0</td>
<td>J8Y09DXC</td>
<td>system-1 (118065481)</td>
</tr>
</tbody>
</table>

```

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:
    ```
        metrocluster node show - fields configuration-state
    ```
    Example
    ```
        nodel_siteA::> metrocluster node show -fields configuration-state
        dr-group-id       cluster node       configuration-state
        -----------       ---------------------- -------------- -------------------
        1 nodel_siteA     nodelmcc-001       configured
        1 nodel_siteA     nodelmcc-002       configured
        1 nodel_siteB     nodelmcc-003       configured
        1 nodel_siteB     nodelmcc-004       configured

        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

e. Run Config Advisor. Go to the Config Advisor page on the NetApp Support Site at support.netapp.com/NOW/download/tools/config_advisor/.

   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

**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”

**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 © 1994–2017 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52.227-19 (June 1987).

Trademark information

Active IQ, AltaVault, Arch Design, ASUP, AutoSupport, Campaign Express, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Element, Fitness, Flash Accel, Flash Cache, Flash Pool, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, Fueled by SolidFire, GetSuccessful, Helix Design, LockVault, Manage ONTAP, MetroCluster, MultiStore, NetApp, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANscreen, SANshare, SANtivity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, SolidFire Helix, StorageGRID, SyncMirror, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web.


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.
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., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277