Replacing the boot media

The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots. Depending on your network configuration, you can perform either a nondisruptive or disruptive replacement.

Before you begin

You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the image_xxx.tgz.

About this task

• The nondisruptive and disruptive methods for replacing a boot media both require you to restore the var file system:
  ◦ For nondisruptive replacement, the HA pair must be connected to a network to restore the var file system.
  ◦ For disruptive replacement, you do not need a network connection to restore the var file system, but the process requires two reboots.
• You must replace the failed component with a replacement FRU component you received from your provider.
• It is important that you apply the commands in these steps on the correct node:
  ◦ The impaired node is the node on which you are performing maintenance.
  ◦ The healthy node is the HA partner of the impaired node.

Steps

1. Shutting down the impaired controller on page 1
2. Shutting down the node on page 2
3. Shutting down a node in a two-node MetroCluster configuration running ONTAP on page 2
4. Opening the controller module on page 4
5. Replacing the boot media on page 5
6. Transferring the boot image to the boot media on page 6
7. Healing and switching back aggregates in a two-node MetroCluster configuration on page 9
8. Completing the replacement process on page 11

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.

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 <strong>y</strong> when prompted.</td>
</tr>
<tr>
<td>System prompt or password prompt</td>
<td>Take over or halt the impaired node:</td>
</tr>
<tr>
<td></td>
<td>- For an HA pair, take over the impaired node from the healthy node:</td>
</tr>
</tbody>
</table>
   |                                      |     ```bash
   |                                      |     storage failover takeover -ofnode impaired_node_name
   |                                      |     ``` |
   |                                      | When the impaired node shows Waiting for giveback..., press Ctrl-C, and then respond **y**. |

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:
   ```bash
   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>
</tbody>
</table>
If the impaired node... Then...

| Has not automatically switched over | Perform a planned switchover operation from the healthy node:  
| metrocluster switchover |
| Has not automatically switched over and planned switchover with the | 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.

Example

controller_A_1::> metrocluster operation show  
Operation: heal-aggregates  
State: successful  
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

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

**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. 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.

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

Replacing the boot media

You must locate the boot media in the controller and follow the directions to replace it.

Steps
1. If you are not already grounded, properly ground yourself.
2. Locate the boot media using the following illustration or the FRU map on the controller module:

3. 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.

4. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.

5. 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.

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

7. Close the controller module cover.

Transferring the boot image to the boot media

You can install the system image to the replacement boot media using a USB flash drive with the image installed on it. However, you must restore the \texttt{var} file system during this procedure.

Before you begin

You must have a USB flash drive, formatted to FAT32, with the following items:

- A copy of the same image version of ONTAP as what the impaired controller was running.
  You can download the appropriate image from the Downloads section on the NetApp Support Site.
- If your system is an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the \texttt{var} file system.

Steps

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

2. Reinstall the cable management device and recable the system, as needed.
   When recabling, remember to reinstall the media converters (SFPs) if they were removed.

3. Insert the USB flash drive into the USB slot on the controller module.
   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, push the cam handle to the closed position, and then tighten the thumbscrew.
   The node begins to boot as soon as it is completely installed into the chassis.

5. Interrupt the boot process to stop at the LOADER prompt by pressing \texttt{Ctrl-C} when you see \texttt{Starting AUTOBOOT press Ctrl-C to abort...}.
   If you miss this message, press \texttt{Ctrl-C}, select the option to boot to Maintenance mode, and then \texttt{halt} the node to boot to LOADER.

6. For systems with one controller in the chassis, reconnect the power and turn on the power supplies.
   The system begins to boot and stops at the LOADER prompt.

7. For systems running ONTAP 9.3 and earlier, verify that the environment variables are set as expected:
   \textbf{Note:} If you are running ONTAP 9.4 or later, the environment variables are persistent and should be set correctly. However, it is a best practice to verify the settings once your system has been restored.
a. From the LOADER prompt, verify that the environment variables are set as expected:

    printenv
    
    • For AFF systems, make sure that `bootarg.init.flash_optimized` is set to `true`. If necessary, reset it by using the `setenv` command.

    • For systems using Storage Encryption (NSE), make sure that `bootarg.storageencryption.support` is set to `true`. If necessary, reset it by using the `setenv` command.

    If you are using KMIP servers, make sure that the `kmip.int.*` variables are properly set, usually during boot.

    ONTAP 9 Disks and Aggregates Power Guide

    • For systems using UTA2 adapters, make sure that the card settings by using the `ucadmin` command, and then make any necessary changes by using the `ucadmin modify` command.

b. If necessary, reset any environment variables:

    setenv environment_variable_name changed_value

   c. Save any changes you made:

    saveenv

8. Set your network connection type at the LOADER prompt:

   • If you are configuring DHCP:

     ifconfig e0a -auto

     Note: The target port you configure is the target port you use to communicate with the impaired node from the healthy node during `var` file system restore with a network connection. You can also use the e0M port in this command.

   • If you are configuring manual connections:

     ifconfig e0a -addr=timer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain

     ◦ `timer_addr` is the IP address of the storage system.

     ◦ `netmask` is the network mask of the management network that is connected to the HA partner.

     ◦ `gateway` is the gateway for the network.

     ◦ `dns_addr` is the IP address of a name server on your network.

     ◦ `dns_domain` is the Domain Name System (DNS) domain name.

     If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL. You need only the server’s host name.

     Note: Other parameters might be necessary for your interface. You can enter `help ifconfig` at the firmware prompt for details.

9. Boot the recovery image:

    boot_recovery ontap_image_name.tgz

    Note: If the `image.tgz` file is named something other than `image.tgz`, such as `boot_recovery 9_4.tgz`, you need to include the different file name in the `boot_recovery` command.

    The system boots to the boot menu and prompts you for the boot image name.

10. Enter the boot image name that is on the USB flash drive:

    image_name.tgz

    After `image_name.tgz` is installed, the system prompts you to restore the backup configuration (the `var` file system) from the healthy node.
11. **Restore the var file system:**

<table>
<thead>
<tr>
<th>If your system has...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| A network connection   | a. Press `y` when prompted to restore the backup configuration.  
                          | b. Set the healthy node to advanced privilege level:  
                          | `set -privilege advanced`  
                          | c. Run the restore backup command:  
                          | `system node restore-backup -node local -target-address impaired_node_IP_address`  
                          | d. Return the node to admin level:  
                          | `set -privilege admin`  
                          | e. Press `y` when prompted to use the restored configuration.  
                          | f. Press `y` when prompted to reboot the node. |
| No network connection  | a. Press `n` when prompted to restore the backup configuration.  
                          | b. Reboot the system when prompted by the system.  
                          | c. Select the **Update flash from backup config** (sync flash) option from the displayed menu.  
                          | If you are prompted to continue with the update, press `y`. |

12. Although ONTAP 9.4 retains the environment variable settings, it is a best practice to verify that they are set as expected.

   a. Take the node to the LOADER prompt.
   
   b. Check the environment variable settings with the `printenv` command.
   
   c. If an environment variable is not set as expected, modify it with the `setenv environment_variable_name changed_value` command.
   
   d. Save your changes using the `saveenv` command.
   
   e. Reboot the node.

13. The next step depends on your system configuration:

<table>
<thead>
<tr>
<th>If your system is in...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A stand-alone configuration</td>
<td>You can begin using your system after the node reboots.</td>
</tr>
</tbody>
</table>
If your system is in... | Then...
---|---
An HA pair | After the impaired node is displaying the Waiting for Giveback... message, perform a giveback from the healthy node:
   a. Perform a giveback from the healthy node:
      ```
      storage failover giveback -ofnode partner_node_name
      ```
      This initiates the process of returning ownership of the impaired node's aggregates and volumes from the healthy node back to the impaired node.
      **Note:** If the giveback is vetoed, you can consider overriding the vetoes.
   b. Monitor the progress of the giveback operation by using the `storage failover show-giveback` command.
   c. After the giveback operation is complete, confirm that the HA pair is healthy and that takeover is possible by using the `storage failover show` command.
   d. Restore automatic giveback if you disabled it by using the `storage failover modify` command.

A two-node MetroCluster configuration | Proceed to the next step.
| The MetroCluster healing and switchback procedures are done in the next task in the replacement process.

### 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.
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     Configuration  DR State          Mirroring Mode
----- ------- -------------- -------------- --------- --------------------
1     cluster_A controller_A_1 configured enabled heal roots completed
2     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:

```
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.

**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**

Copyright © 2019 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

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