



Maintain

Install and maintain

NetApp
February 02, 2026

Table of Contents

- Maintain 1
 - Maintain AFF A700 hardware 1
 - Boot media 1
 - Caching module 1
 - Chassis 1
 - Controller 1
 - DCPM 1
 - DIMM 1
 - Fan 1
 - I/O module 1
 - LED USB 1
 - NVRAM 2
 - Power supply 2
 - Real-time clock battery 2
 - X91148A module 2
 - Boot media 2
 - Overview of boot media replacement - AFF A700 2
 - Check encryption key support and status - AFF A700 3
 - Shut down the impaired controller - AFF A700 6
 - Replace the boot media - AFF A700 9
 - Boot the recovery image - AFF A700 13
 - Switch back aggregates in a two-node MetroCluster configuration - AFF A700 17
 - Restore encryption - AFF A700 18
 - Return the failed part to NetApp - AFF A700 28
 - Chassis 28
 - Overview of chassis replacement - AFF A700 28
 - Shut down the controllers - AFF A700 29
 - Move and replace hardware - AFF A700 32
 - Complete the restoration and replacement process - AFF A700 39
 - Controller module 41
 - Overview of controller module replacement - AFF A700 41
 - Shut down the impaired controller - AFF 700 42
 - Replace the controller module hardware - AFF A700 46
 - Restore and verify the system configuration - AFF A700 51
 - Recable the system and reassign disks - AFF A700 52
 - Complete system restoration - AFF A700 58
 - Hot-swap a de-stage controller power module (DCPM) - AFF A700 61
 - Step 1: Replace the DCPM module 61
 - Step 2: Dispose of batteries 62
 - Step 3: Return the failed part to NetApp 62
 - Replace a DIMM - AFF A700 62
 - Step 1: Shut down the impaired controller 63
 - Step 2: Remove the controller module 67

Step 3: Replace the DIMMs	68
Step 4: Install the controller	71
Step 5: Switch back aggregates in a two-node MetroCluster configuration.	71
Step 6: Return the failed part to NetApp	73
Swap out a fan - AFF A700	73
Replace an I/O module - AFF A700 and FAS9000.	74
Step 1: Shut down the impaired controller	74
Step 2: Replace I/O modules	78
Step 3: Reboot the controller after I/O module replacement	79
Step 4: Switch back aggregates in a two-node MetroCluster configuration.	79
Step 5: Return the failed part to NetApp	81
Replace an LED USB module - AFF A700.	81
Return the failed part to NetApp.	82
Replace the NVRAM module or NVRAM DIMMs - AFF A700	82
Step 1: Shut down the impaired controller	82
Step 2: Replace the NVRAM module.	86
Step 3: Replace a NVRAM DIMM	88
Step 4: Reboot the controller after FRU replacement	90
Step 5: Reassign disks.	90
Step 6: Return the failed part to NetApp	96
Hot-swap a power supply - AFF A700	96
Replace the real-time clock battery - AFF 700	98
Step 1: Shut down the impaired controller	98
Step 2: Remove the controller module	102
Step 3: Replace the RTC battery	103
Step 4: Reinstall the controller module and set time/date	104
Step 5: Switch back aggregates in a two-node MetroCluster configuration.	105
Step 6: Return the failed part to NetApp	107
X91148A module	107
Overview of adding an X91148A module - AFF A700	107
Add an X91148A module in a system with open slots - A700	107
Add an X91148A storage module in a system with no open slots - A700	109

Maintain

Maintain AFF A700 hardware

For the AFF A700 storage system, you can perform maintenance procedures on the following components.

Boot media

The boot media stores a primary and secondary set of boot image files that the system uses when it boots. The AFF A700 and FAS9000 system supports only manual boot media recovery procedures.

Caching module

You must replace the controller's caching module when your system registers a single AutoSupport (ASUP) message that the module has gone offline.

Chassis

The chassis is the physical enclosure housing all the controller components such as the controller/CPU unit, power supply, and I/O.

Controller

A controller consists of a board, firmware, and software. It controls the drives and implements the ONTAP functions.

DCPM

The DCPM (destage controller power module) contains the NVRAM11 battery.

DIMM

You must replace a DIMM (dual in-line memory module) when a memory mismatch is present, or you have a failed DIMM.

Fan

The fan cools the controller.

I/O module

The I/O module (Input/Output module) is a hardware component that acts as an intermediary between the controller and various devices or systems that need to exchange data with the controller.

LED USB

The LED USB module provides connectivity to console ports and system status.

NVRAM

The NVRAM module (Non-Volatile Random Access Memory) allows the controller to retain data across power cycles or system reboots.

Power supply

A power supply provides a redundant power source in a controller shelf.

Real-time clock battery

A real time clock battery preserves system date and time information if the power is off.

X91148A module

The X91148A module is an I/O module that acts as an intermediary between the controller and various devices or systems that need to exchange data with the controller.

Boot media

Overview of boot media replacement - AFF A700

Learn about boot media replacement on an AFF A700 system and understand the different replacement methods. The boot media stores primary and secondary boot image files that the system uses during startup. Depending on your network configuration, you can perform either a nondisruptive replacement (using internal e0S connection) or a disruptive replacement (requires two reboots).

The AFF A700 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

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.

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

You also must copy the `image_XXX.tgz` file to the USB flash drive for later use in this procedure.

- 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 does not require connection to a network to restore the `var` file system. The HA pair in a single chassis has an internal e0S connection, which is used to transfer `var` config between them.
 - 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.

Check encryption key support and status - AFF A700

To ensure data security on your storage system, you need to verify the encryption key support and status on your boot media. The AFF A700 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

Check if your ONTAP version supports NetApp Volume Encryption (NVE), and before you shut down the controller check if the key manager is active.

Step 1: Check NVE support and download the correct ONTAP image

Determine whether your ONTAP version supports NetApp Volume Encryption (NVE) so you can download the correct ONTAP image for the boot media replacement.

Steps

1. Check if your ONTAP version supports encryption:

```
version -v
```

If the output includes `1Ono-DARE`, NVE is not supported on your cluster version.

2. Download the appropriate ONTAP image based on NVE support:
 - If NVE is supported: Download the ONTAP image with NetApp Volume Encryption
 - If NVE is not supported: Download the ONTAP image without NetApp Volume Encryption



Download the ONTAP image from the NetApp Support Site to your HTTP or FTP server or a local folder. You will need this image file during the boot media replacement procedure.

Step 2: Verify key manager status and back up configuration

Before shutting down the impaired controller, verify the key manager configuration and back up the necessary information.

Steps

1. Determine which key manager is enabled on your system:

ONTAP version	Run this command
ONTAP 9.14.1 or later	<pre>security key-manager keystore show</pre> <ul style="list-style-type: none"> • If EKM is enabled, <code>EKM</code> is listed in the command output. • If OKM is enabled, <code>OKM</code> is listed in the command output. • If no key manager is enabled, <code>No key manager keystores configured</code> is listed in the command output.
ONTAP 9.13.1 or earlier	<pre>security key-manager show-key-store</pre> <ul style="list-style-type: none"> • If EKM is enabled, <code>external</code> is listed in the command output. • If OKM is enabled, <code>onboard</code> is listed in the command output. • If no key manager is enabled, <code>No key managers configured</code> is listed in the command output.

2. Depending on whether a key manager is configured on your system, do one of the following:

If no key manager is configured:

You can safely shut down the impaired controller and proceed to the shutdown procedure.

If a key manager is configured (EKM or OKM):

- a. Enter the following query command to display the status of the authentication keys in your key manager:

```
security key-manager key query
```

- b. Review the output and check the value in the `Restored` column. This column indicates whether the authentication keys for your key manager (either EKM or OKM) have been successfully restored.

3. Complete the appropriate procedure based on your key manager type:

External Key Manager (EKM)

Complete these steps based on the value in the `Restored` column.

If all keys show `true` in the `Restored` column:

You can safely shut down the impaired controller and proceed to the shutdown procedure.

If any keys show a value other than `true` in the `Restored` column:

- a. Restore the external key management authentication keys to all nodes in the cluster:

```
security key-manager external restore
```

If the command fails, contact NetApp Support.

- b. Verify that all authentication keys are restored:

```
security key-manager key query
```

Confirm that the `Restored` column displays `true` for all authentication keys.

- c. If all keys are restored, you can safely shut down the impaired controller and proceed to the shutdown procedure.

Onboard Key Manager (OKM)

Complete these steps based on the value in the `Restored` column.

If all keys show `true` in the `Restored` column:

- a. Back up the OKM information:

- i. Switch to advanced privilege mode:

```
set -priv advanced
```

Enter `y` when prompted to continue.

- ii. Display the key management backup information:

```
security key-manager onboard show-backup
```

- iii. Copy the backup information to a separate file or your log file.

You will need this backup information if you need to manually recover OKM during the replacement procedure.

- iv. Return to admin mode:

```
set -priv admin
```

- b. You can safely shut down the impaired controller and proceed to the shutdown procedure.

If any keys show a value other than `true` in the `Restored` column:

a. Synchronize the onboard key manager:

```
security key-manager onboard sync
```

Enter the 32-character alphanumeric onboard key management passphrase when prompted.



This is the cluster-wide passphrase you created when you initially configured the Onboard Key Manager. If you do not have this passphrase, contact NetApp Support.

b. Verify all authentication keys are restored:

```
security key-manager key query
```

Confirm that the `Restored` column displays `true` for all authentication keys and the `Key Manager type` shows `onboard`.

c. Back up the OKM information:

i. Switch to advanced privilege mode:

```
set -priv advanced
```

Enter `y` when prompted to continue.

ii. Display the key management backup information:

```
security key-manager onboard show-backup
```

iii. Copy the backup information to a separate file or your log file.

You will need this backup information if you need to manually recover OKM during the replacement procedure.

iv. Return to admin mode:

```
set -priv admin
```

d. You can safely shut down the impaired controller and proceed to the shutdown procedure.

Shut down the impaired controller - AFF A700

Shut down the impaired controller on an AFF A700 system after completing encryption checks. This procedure includes taking the controller to the `LOADER` prompt, capturing boot environmental variables for reference, and preparing the controller for boot media replacement, with specific steps that vary depending on your system configuration.

The AFF A700 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

Option 1: Most systems

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.

Steps

- a. Take the impaired controller to the LOADER prompt:

If the impaired controller displays...	Then...
The LOADER prompt	Go to Remove controller module.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: <pre>storage failover takeover -ofnode impaired_node_name</pre> When the impaired controller shows Waiting for giveback..., press Ctrl-C, and then respond <code>y</code> .

- b. From the LOADER prompt, enter: `printenv` to capture all boot environmental variables. Save the output to your log file.



This command may not work if the boot device is corrupted or non-functional.

Option 2: Controller is in a MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired node. NOTE: Do not use this procedure if your system is in a two-node MetroCluster configuration.

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

- 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 controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see [Synchronize a node with the cluster](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message  
MAINT=number_of_hours_downh
```

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*>`

```
system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt (enter system password)	Take over or halt the impaired controller from the healthy controller: <code>storage failover takeover -ofnode impaired_node_name</code> When the impaired controller shows Waiting for giveback..., press Ctrl-C, and then respond <code>y</code> .

Option 3: Controller is in a two-node MetroCluster

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired node.



Do not use this procedure if your system is in a two-node MetroCluster configuration.

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

- 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 controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see [Synchronize a node with the cluster](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message  

MAINT=number_of_hours_downh
```

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*>`

```
system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.

If the impaired controller is displaying...	Then...
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt (enter system password)	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name</pre> <p>When the impaired controller shows Waiting for giveback..., press Ctrl-C, and then respond <code>y</code>.</p>

Replace the boot media - AFF A700

Replace the failed boot media on an AFF A700 controller module. This procedure includes removing the controller module from the chassis, physically replacing the boot media component, transferring the boot image to the replacement media using a USB flash drive, and restoring the system to normal operation.

The AFF A700 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

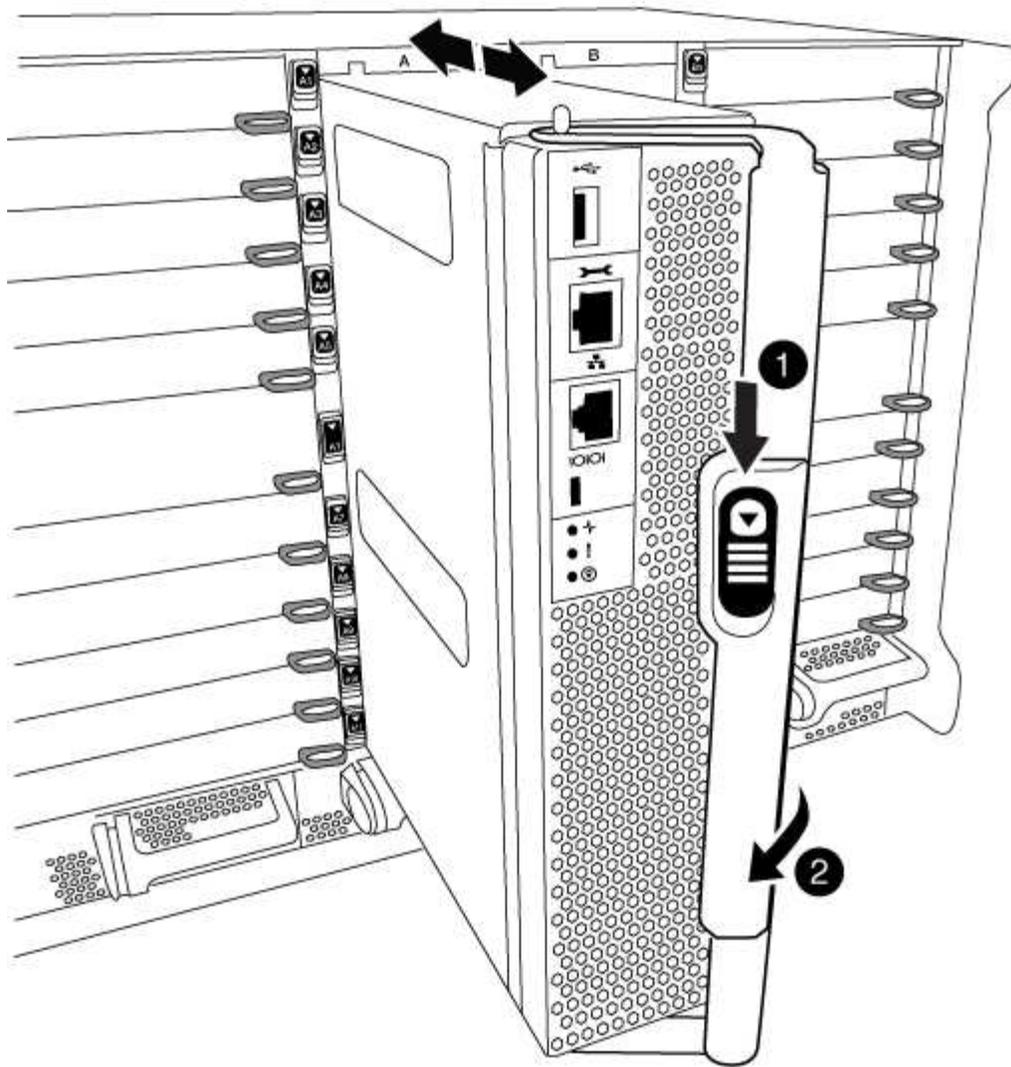
To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

Step 1: Remove the controller

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

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

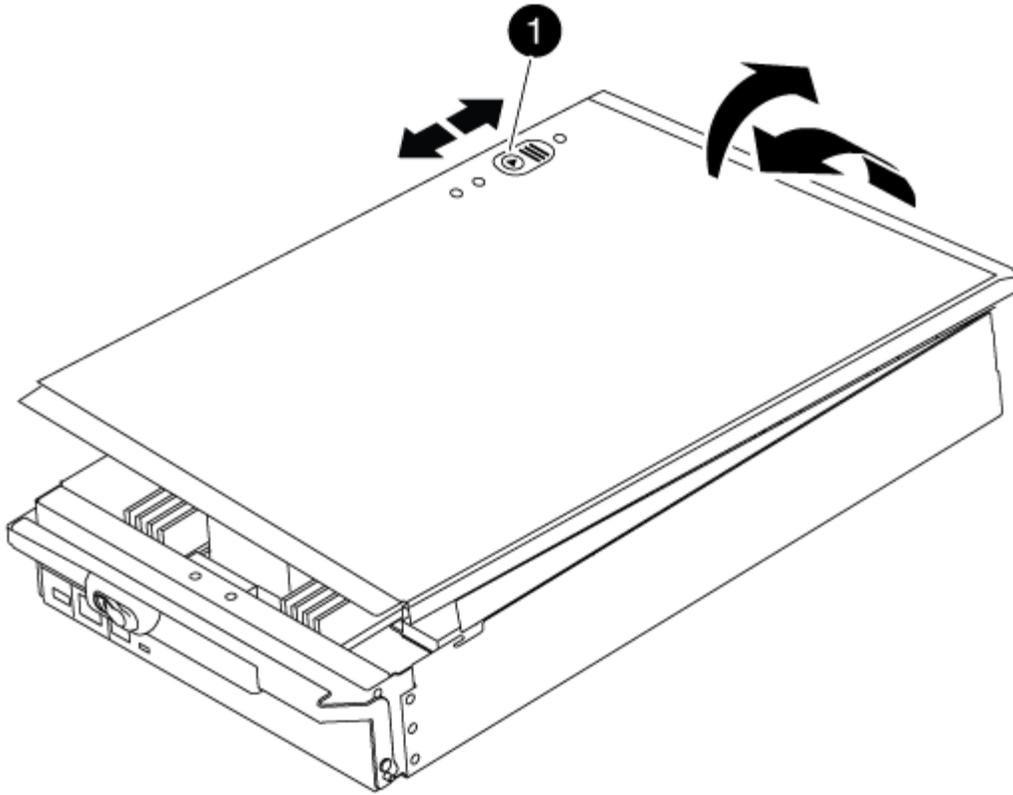


1	
	Cam handle release button
2	
	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

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

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

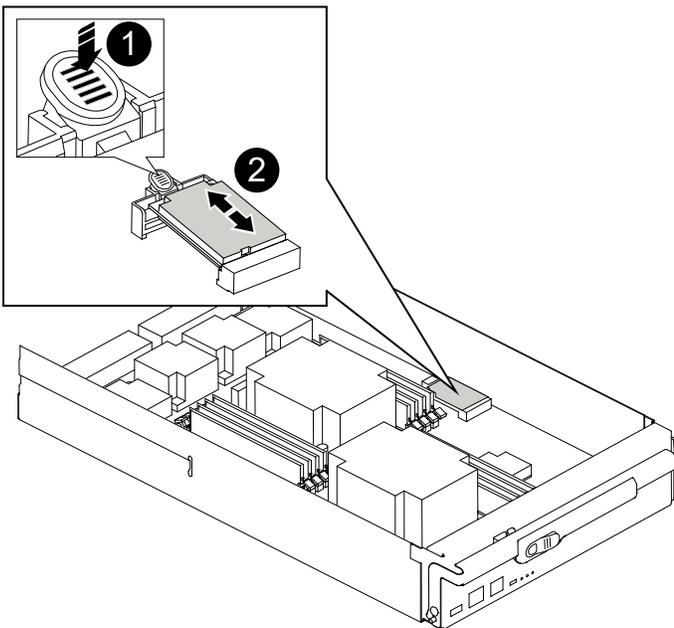


1

Controller module cover locking button

Step 2: Replace the boot media

Locate the boot media using the following illustration or the FRU map on the controller module:



1

Press release tab

2

Boot media

1. 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.



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

2. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
3. Check the boot media to make sure that it is seated squarely and completely in the socket.

If necessary, remove the boot media and reseal it into the socket.

4. Push the boot media down to engage the locking button on the boot media housing.
5. Reinstall the controller module lid by aligning the pins on the lid with the slots on the motherboard carrier, and then slide the lid into place.

Step 3: Transfer 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 `var` file system during this procedure.

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.
- 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 NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
 - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- 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 `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. Recable the controller module, as needed.
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, and then push the cam handle to the closed position.

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 Ctrl-C when you see Starting AUTOBOOT press Ctrl-C to abort....

If you miss this message, press Ctrl-C, select the option to boot to Maintenance mode, and then halt the node to boot to LOADER.

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

- If you are configuring DHCP: `ifconfig e0a -auto`



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=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
 - `filer_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.



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

7. If the controller is in a stretch or fabric-attached MetroCluster, you must restore the FC adapter configuration:

- a. Boot to Maintenance mode: `boot_ontap maint`
- b. Set the MetroCluster ports as initiators: `ucadmin modify -m fc -t initiator adapter_name`
- c. Halt to return to Maintenance mode: `halt`

The changes will be implemented when the system is booted.

Boot the recovery image - AFF A700

Boot the ONTAP recovery image from the USB drive on an AFF A700 system to restore the boot media. This procedure includes booting from the USB flash drive, restoring the

file system, verifying environmental variables, and returning the controller to normal operation, with specific steps that vary depending on whether the system is in a two-node MetroCluster configuration.

The AFF A700 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

The procedure for booting the impaired node from the recovery image depends on whether the system is in a two-node MetroCluster configuration.

Option 1: Boot the recovery image in most systems

You must boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

This procedure applies to systems that are not in a two-node MetroCluster configuration.

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.
3. Restore the `var` file system:

If your system has...	Then...
A network connection	<ol style="list-style-type: none"> a. Press <code>y</code> when prompted to restore the backup configuration. b. Set the healthy node to advanced privilege level: <code>set -privilege advanced</code> c. Run the restore backup command: <code>system node restore-backup -node local -target-address <i>impaired_node_IP_address</i></code> d. Return the node to admin level: <code>set -privilege admin</code> e. Press <code>y</code> when prompted to use the restored configuration. f. Press <code>y</code> when prompted to reboot the node.
No network connection	<ol style="list-style-type: none"> a. Press <code>n</code> 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. <p>If you are prompted to continue with the update, press <code>y</code>.</p>

If your system has...	Then...
No network connection and is in a MetroCluster IP configuration	<p>a. Press <code>n</code> when prompted to restore the backup configuration.</p> <p>b. Reboot the system when prompted by the system.</p> <p>c. Wait for the iSCSI storage connections to connect.</p> <p>You can proceed after you see the following messages:</p> <pre data-bbox="672 394 1489 1255"> date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address). </pre> <p>d. Select the Update flash from backup config (sync flash) option from the displayed menu.</p> <p>If you are prompted to continue with the update, press <code>y</code>.</p>

4. Ensure that the environmental variables 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 `savenv` command.

5. The next depends on your system configuration:

- If your system has onboard keymanager, NSE or NVE configured, go to [Restore OKM, NSE, and NVE as needed](#)

- If your system does not have onboard keymanager, NSE or NVE configured, complete the steps in this section.

6. From the LOADER prompt, enter the `boot_ontap` command.

If you see...	Then...
The login prompt	Go to the next Step.
Waiting for giveback...	a. Log into the partner node. b. Confirm the target node is ready for giveback with the <code>storage failover show</code> command.

7. Connect the console cable to the partner node.

8. Give back the node using the `storage failover giveback -fromnode local` command.

9. At the cluster prompt, check the logical interfaces with the `net int -is-home false` command.

If any interfaces are listed as "false", revert those interfaces back to their home port using the `net int revert` command.

10. Move the console cable to the repaired node and run the `version -v` command to check the ONTAP versions.

11. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

Option 2: Boot the recovery image in a two-node MetroCluster configuration

You must boot the ONTAP image from the USB drive and verify the environmental variables.

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

Steps

1. From the LOADER prompt, boot the recovery image from the USB flash drive: `boot_recovery`

The image is downloaded from the USB flash drive.

2. When prompted, either enter the name of the image or accept the default image displayed inside the brackets on your screen.

3. After the image is installed, start the restoration process:

a. Press `n` when prompted to restore the backup configuration.

b. Press `y` when prompted to reboot to start using the newly installed software.

You should be prepared to interrupt the boot process when prompted.

4. As the system boots, press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message., and when the Boot Menu is displayed select option 6.

5. Verify that the environmental variables 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 `savenv` command.
- e. Reboot the node.

Switch back aggregates in a two-node MetroCluster configuration - AFF A700

After completing the boot media replacement, perform the MetroCluster switchback operation. The AFF A700 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the enabled state: `metrocluster node show`

```
cluster_B::> metrocluster node show

DR                               Configuration  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.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

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.

6. Reestablish any SnapMirror or SnapVault configurations.

Restore encryption - AFF A700

Restore encryption on the replacement boot media. The AFF A700 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

Complete the appropriate steps to restore encryption on your system based on your key manager type. If you are unsure which key manager your system uses, check the settings you captured at the beginning of the boot media replacement procedure.

Onboard Key Manager (OKM)

Restore the Onboard Key Manager (OKM) configuration from the ONTAP boot menu.

Before you begin

Ensure you have the following information available:

- Cluster-wide passphrase entered while [enabling onboard key management](#)
- [Backup information for the Onboard Key Manager](#)
- Verification that you have the correct passphrase and backup data using the [How to verify onboard key management backup and cluster-wide passphrase](#) procedure

Steps

On the impaired controller:

1. Connect the console cable to the impaired controller.
2. From the ONTAP boot menu, select the appropriate option:

ONTAP version	Select this option
ONTAP 9.8 or later	<p>Select option 10.</p> <p>Show example boot menu</p> <div style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"><p>Please choose one of the following:</p><ul style="list-style-type: none">(1) Normal Boot.(2) Boot without /etc/rc.(3) Change password.(4) Clean configuration and initialize all disks.(5) Maintenance mode boot.(6) Update flash from backup config.(7) Install new software first.(8) Reboot node.(9) Configure Advanced Drive Partitioning.(10) Set Onboard Key Manager recovery secrets.(11) Configure node for external key management.<p>Selection (1-11)? 10</p></div>

ONTAP version	Select this option
ONTAP 9.7 and earlier	<p data-bbox="634 155 1377 191">Select the hidden option <code>recover_onboard_keymanager</code></p> <p data-bbox="634 226 959 262">Show example boot menu</p> <div data-bbox="667 304 1422 968" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p data-bbox="695 338 1305 369">Please choose one of the following:</p> <ul style="list-style-type: none"> <li data-bbox="699 417 987 449">(1) Normal Boot. <li data-bbox="699 457 1146 489">(2) Boot without <code>/etc/rc</code>. <li data-bbox="699 497 1057 529">(3) Change password. <li data-bbox="695 537 1377 606">(4) Clean configuration and initialize all disks. <li data-bbox="699 615 1162 646">(5) Maintenance mode boot. <li data-bbox="699 655 1338 686">(6) Update flash from backup config. <li data-bbox="699 695 1252 726">(7) Install new software first. <li data-bbox="699 735 987 766">(8) Reboot node. <li data-bbox="695 774 1203 844">(9) Configure Advanced Drive Partitioning. <p data-bbox="695 852 992 884">Selection (1-19)?</p> <p data-bbox="695 892 1149 924"><code>recover_onboard_keymanager</code></p> </div>

3. Confirm that you want to continue the recovery process when prompted:

Show example prompt

```
This option must be used only in disaster recovery procedures. Are you
sure? (y or n):
```

4. Enter the cluster-wide passphrase twice.

While entering the passphrase, the console does not show any input.

Show example prompt

```
Enter the passphrase for onboard key management:
Enter the passphrase again to confirm:
```

5. Enter the backup information:

- a. Paste the entire content from the BEGIN BACKUP line through the END BACKUP line, including the dashes.


```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
-----END
BACKUP-----
```

b. Press Enter twice at the end of the input.

The recovery process completes and displays the following message:

Successfully recovered keymanager secrets.

Show example prompt

```
Trying to recover keymanager secrets....
Setting recovery material for the onboard key manager
Recovery secrets set successfully
Trying to delete any existing km_onboard.wkeydb file.

Successfully recovered keymanager secrets.

*****
*****
* Select option "(1) Normal Boot." to complete recovery
process.
*
* Run the "security key-manager onboard sync" command to
synchronize the key database after the node reboots.
*****
*****
```



Do not proceed if the displayed output is anything other than Successfully recovered keymanager secrets. Perform troubleshooting to correct the error.

6. Select option 1 from the boot menu to continue booting into ONTAP.

Show example prompt

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery
process.
*
*****
*****

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

7. Confirm that the controller's console displays the following message:

```
Waiting for giveback...(Press Ctrl-C to abort wait)
```

On the partner controller:

8. Giveback the impaired controller:

```
storage failover giveback -fromnode local -only-cfo-aggregates true
```

On the impaired controller:

9. After booting with only the CFO aggregate, synchronize the key manager:

```
security key-manager onboard sync
```

10. Enter the cluster-wide passphrase for the Onboard Key Manager when prompted.

Show example prompt

```
Enter the cluster-wide passphrase for the Onboard Key Manager:
```

```
All offline encrypted volumes will be brought online and the corresponding volume encryption keys (VEKs) will be restored automatically within 10 minutes. If any offline encrypted volumes are not brought online automatically, they can be brought online manually using the "volume online -vserver <vserver> -volume <volume_name>" command.
```



If the sync is successful, the cluster prompt is returned with no additional messages. If the sync fails, an error message appears before returning to the cluster prompt. Do not continue until the error is corrected and the sync runs successfully.

11. Verify that all keys are synced:

```
security key-manager key query -restored false
```

The command should return no results. If any results appear, repeat the sync command until no results are returned.

On the partner controller:

12. Giveback the impaired controller:

```
storage failover giveback -fromnode local
```

13. Restore automatic giveback if you disabled it:

```
storage failover modify -node local -auto-giveback true
```

14. If AutoSupport is enabled, restore automatic case creation:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

External Key Manager (EKM)

Restore the External Key Manager configuration from the ONTAP boot menu.

Before you begin

Gather the following files from another cluster node or from your backup:

- /cfcard/kmip/servers.cfg file or the KMIP server address and port
- /cfcard/kmip/certs/client.crt file (client certificate)
- /cfcard/kmip/certs/client.key file (client key)
- /cfcard/kmip/certs/CA.pem file (KMIP server CA certificates)

Steps

On the impaired controller:

1. Connect the console cable to the impaired controller.
2. Select option 11 from the ONTAP boot menu.

Show example boot menu

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 11
```

3. Confirm you have gathered the required information when prompted:

Show example prompt

```
Do you have a copy of the /cfcard/kmip/certs/client.crt file?
{y/n}
Do you have a copy of the /cfcard/kmip/certs/client.key file?
{y/n}
Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}
Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}
```

4. Enter the client and server information when prompted:
 - a. Enter the client certificate (client.crt) file contents, including the BEGIN and END lines.
 - b. Enter the client key (client.key) file contents, including the BEGIN and END lines.
 - c. Enter the KMIP server CA(s) (CA.pem) file contents, including the BEGIN and END lines.
 - d. Enter the KMIP server IP address.
 - e. Enter the KMIP server port (press Enter to use the default port 5696).

Show example

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Enter the IP address for the KMIP server: 10.10.10.10
Enter the port for the KMIP server [5696]:

System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
kmip_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmip_init: cmd: ReleaseExtraBSDPort e0M
```

The recovery process completes and displays the following message:

```
Successfully recovered keymanager secrets.
```

Show example

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. Select option 1 from the boot menu to continue booting into ONTAP.

Show example prompt

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery
process.
*
*****
*****

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

6. Restore automatic giveback if you disabled it:

```
storage failover modify -node local -auto-giveback true
```

7. If AutoSupport is enabled, restore automatic case creation:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Return the failed part to NetApp - AFF A700

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information. The AFF A700 system supports only manual boot media recovery procedures. Automated boot media recovery is not supported.

Chassis

Overview of chassis replacement - AFF A700

All other components in the system must be functioning properly; if not, you must contact technical support.

- You can use this procedure with all versions of ONTAP supported by your system.
- This procedure is disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

Shut down the controllers - AFF A700

To replace the chassis, you must shutdown the controllers.

Option 1: Shut down the controllers

This procedure is for systems with two node configurations. For more information about graceful shutdown when servicing a cluster, see [Gracefully shutdown and power up your storage system Resolution Guide - NetApp Knowledge Base](#).

Before you begin

- Make sure you have the necessary permissions and credentials:
 - Local administrator credentials for ONTAP.
 - BMC accessibility for each controller.
- Make sure you have the necessary tools and equipment for the replacement.
- As a best practice before shutdown, you should:
 - Perform additional [system health checks](#).
 - Upgrade ONTAP to a recommended release for the system.
 - Resolve any [Active IQ Wellness Alerts and Risks](#). Make note of any faults presently on the system, such as LEDs on the system components.

Steps

1. Log into the cluster through SSH or log in from any node in the cluster using a local console cable and a laptop/console.
2. Stop all clients/host from accessing data on the NetApp system.
3. Suspend external backup jobs.
4. If AutoSupport is enabled, suppress case creation and indicate how long you expect the system to be offline:

```
system node autosupport invoke -node * -type all -message "MAINT=2h Replace chassis"
```

5. Identify the SP/BMC address of all cluster nodes:

```
system service-processor show -node * -fields address
```

6. Exit the cluster shell:

```
exit
```

7. Log into SP/BMC over SSH using the IP address of any of the nodes listed in the output from the previous step to monitor progress.

If you are using a console/laptop, log into the controller using the same cluster administrator credentials.

8. Halt the two nodes located in the impaired chassis:

```
system node halt -node <node1>,<node2> -skip-lif-migration-before-shutdown true -ignore-quorum-warnings true -inhibit-takeover true
```



For clusters using SnapMirror synchronous operating in StrictSync mode: `system node halt -node <node1>,<node2> -skip-lif-migration-before-shutdown true -ignore-quorum-warnings true -inhibit-takeover true -ignore-strict -sync-warnings true`

9. Enter **y** for each controller in the cluster when you see:

```
Warning: Are you sure you want to halt node <node_name>? {y|n}:
```

10. Wait for each controller to halt and display the LOADER prompt.

Option 2: Shut down a node in a two-node MetroCluster configuration

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

About this task

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

Steps

1. Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
2. Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller...	Then...
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: <code>metrocluster switchover</code>
Has not automatically switched over, you attempted switchover with the <code>metrocluster switchover</code> command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

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

```
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.

```
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.

```
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.

```
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:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
  State: successful
Start Time: 7/29/2016 20:54:41
End Time: 7/29/2016 20:54:42
Errors: -
```

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

Move and replace hardware - AFF A700

Move the fans, hard drives, and controller module or modules from the impaired chassis to the new chassis, and swap out the impaired chassis from the equipment rack or system cabinet with the new chassis of the same model as the impaired chassis.

Step 1: Remove the power supplies

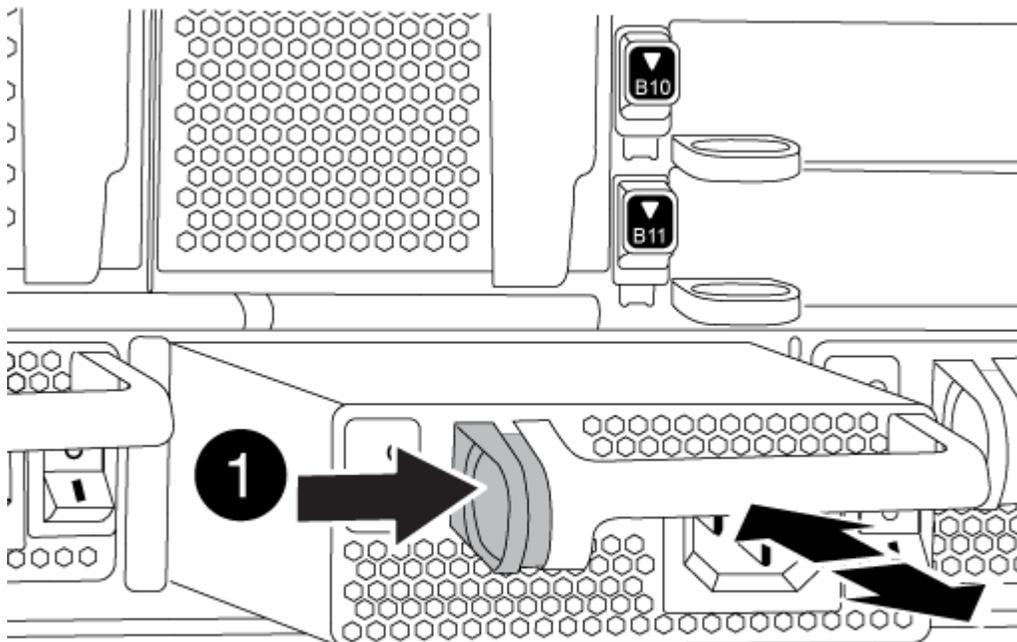
Steps

Removing the power supplies when replacing a chassis involves turning off, disconnecting, and then removing the power supply from the old chassis.

1. If you are not already grounded, properly ground yourself.
2. Turn off the power supply and disconnect the power cables:
 - a. Turn off the power switch on the power supply.
 - b. Open the power cable retainer, and then unplug the power cable from the power supply.
 - c. Unplug the power cable from the power source.
3. Press and hold the orange button on the power supply handle, and then pull the power supply out of the chassis.



When removing a power supply, always use two hands to support its weight.



1	Locking button
----------	----------------

4. Repeat the preceding steps for any remaining power supplies.

Step 2: Remove the fans

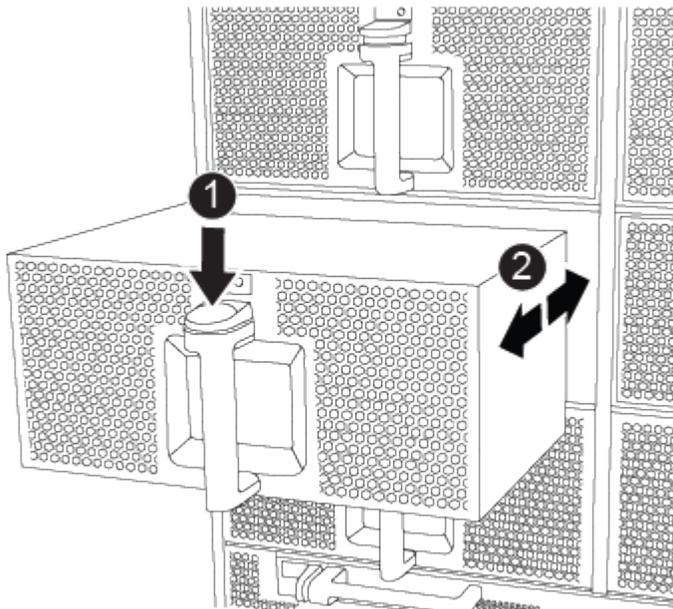
To remove the fan modules when replacing the chassis, you must perform a specific sequence of tasks.

Steps

1. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
2. Press the orange button on the fan module and pull the fan module straight out of the chassis, making sure that you support it with your free hand.



The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.



1	Orange release button
----------	-----------------------

3. Set the fan module aside.
4. Repeat the preceding steps for any remaining fan modules.

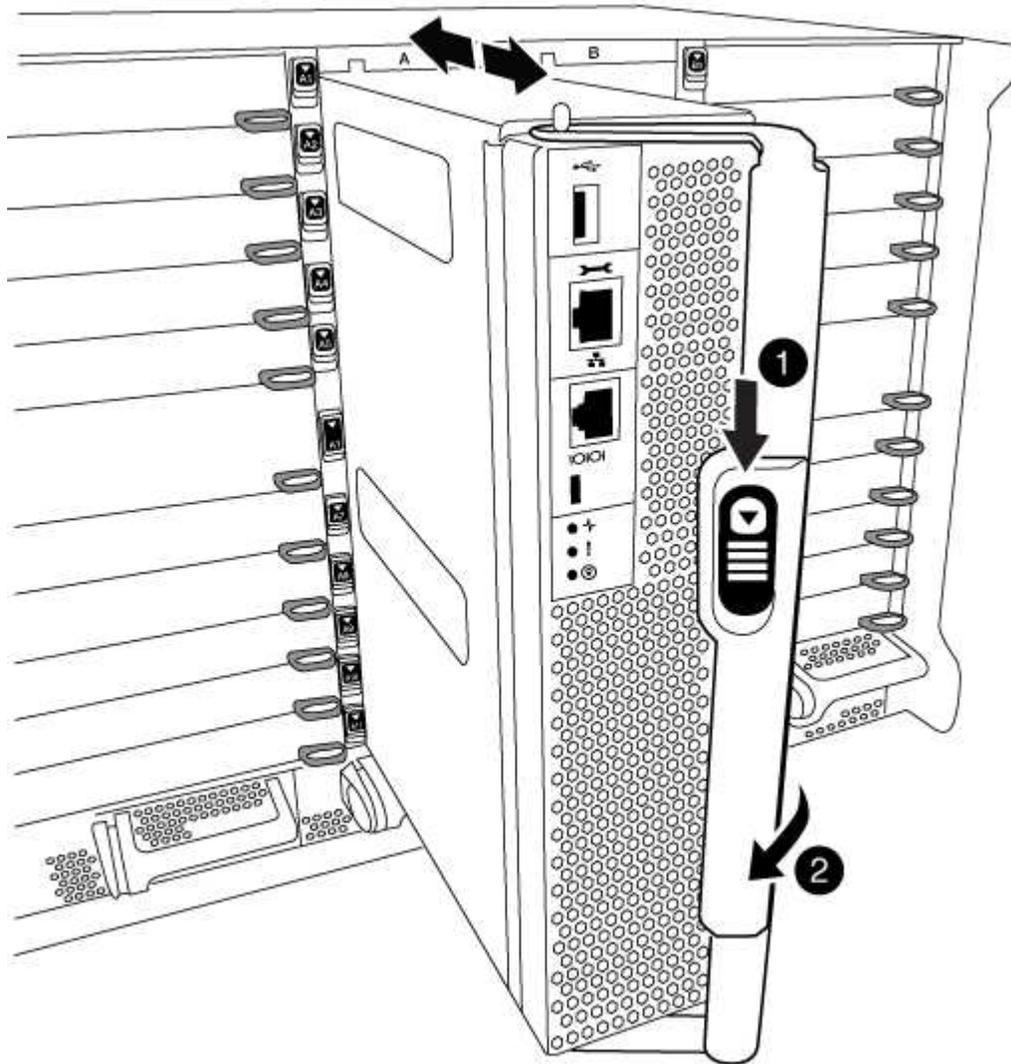
Step 3: Remove the controller module

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

Steps

1. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.

2. Slide the orange button on the cam handle downward until it unlocks.



1	Cam handle release button
2	Cam handle

3. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

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

4. Set the controller module aside in a safe place, and repeat these steps if you have another controller module in the chassis.

Step 4: Remove the I/O modules

Steps

To remove I/O modules from the old chassis, including the NVRAM modules, follow the specific sequence of

steps. You do not have to remove the Flash Cache module from the NVRAM module when moving it to a new chassis.

1. Unplug any cabling associated with the target I/O module.

Make sure that you label the cables so that you know where they came from.

2. Remove the target I/O module from the chassis:

- a. Depress the lettered and numbered cam button.

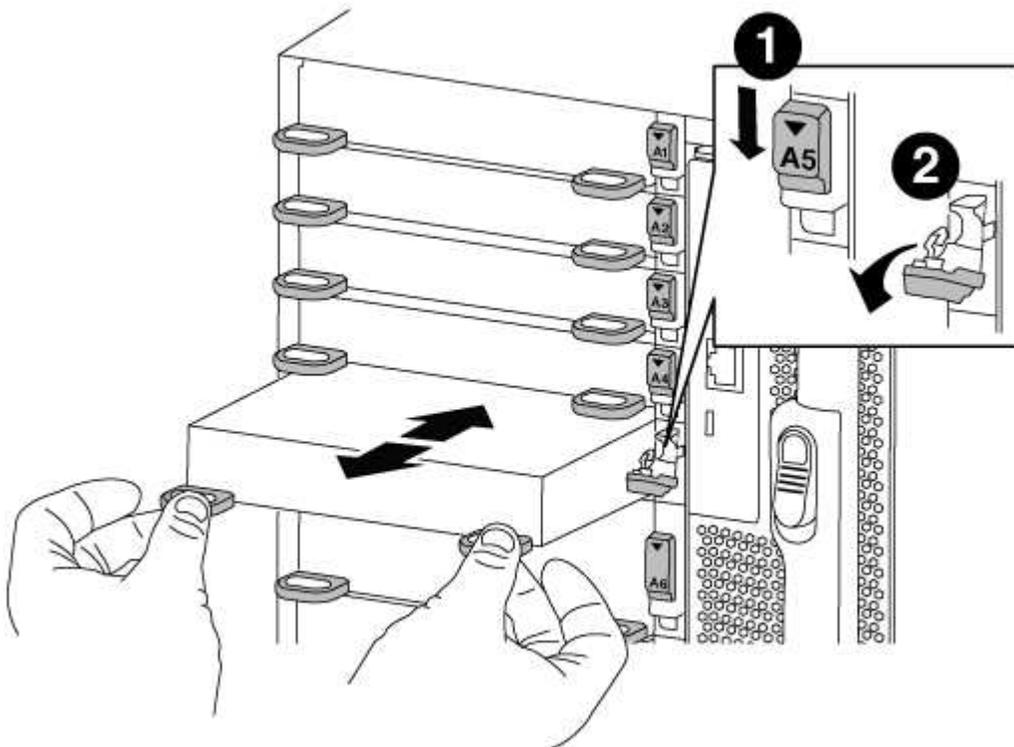
The cam button moves away from the chassis.

- b. Rotate the cam latch down until it is in a horizontal position.

The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

- c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

Make sure that you keep track of which slot the I/O module was in.



1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

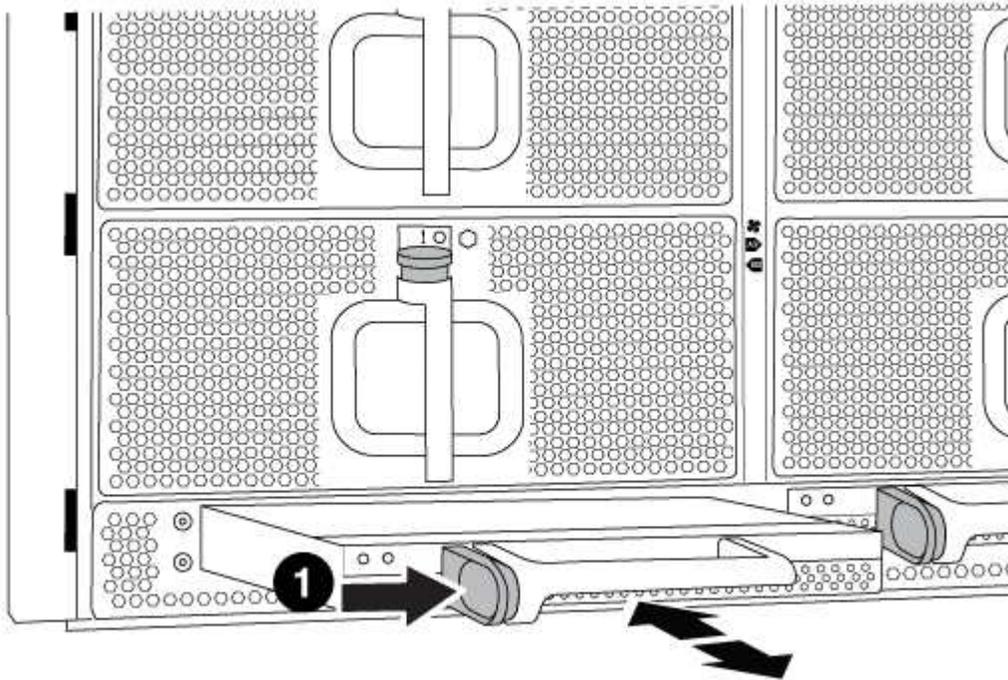
3. Set the I/O module aside.
4. Repeat the preceding step for the remaining I/O modules in the old chassis.

Step 5: Remove the De-stage Controller Power Module

Steps

You must remove the de-stage controller power modules from the old chassis in preparation for installing the replacement chassis.

1. Press the orange locking button on the module handle, and then slide the DCPM module out of the chassis.



1	DCPM module orange locking button
----------	-----------------------------------

2. Set the DCPM module aside in a safe place and repeat this step for the remaining DCPM module.

Step 6: Replace a chassis from within the equipment rack or system cabinet

Steps

You must remove the existing chassis from the equipment rack or system cabinet before you can install the replacement chassis.

1. Remove the screws from the chassis mount points.



If the system is in a system cabinet, you might need to remove the rear tie-down bracket.

2. With the help of two or three people, slide the old chassis off the rack rails in a system cabinet or L brackets in an equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two or three people, install the replacement chassis into the equipment rack or system cabinet by guiding the chassis onto the rack rails in a system cabinet or L brackets in an equipment rack.

5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. Secure the rear of the chassis to the equipment rack or system cabinet.
8. If you are using the cable management brackets, remove them from the old chassis, and then install them on the replacement chassis.
9. If you have not already done so, install the bezel.

Step 7: Move the USB LED module to the new chassis

Steps

Once the new chassis is installed into the rack or cabinet, you must move the USB LED module from the old chassis to the new chassis.

1. Locate the USB LED module on the front of the old chassis, directly under the power supply bays.
2. Press the black locking button on the right side of the module to release the module from the chassis, and then slide it out of the old chassis.
3. Align the edges of the module with the USB LED bay at the bottom-front of the replacement chassis, and gently push the module all the way into the chassis until it clicks into place.

Step 8: Install the de-stage controller power module when replacing the chassis

Steps

Once the replacement chassis is installed into the rack or system cabinet, you must reinstall the de-stage controller power modules into it.

1. Align the end of the DCPM module with the chassis opening, and then gently slide it into the chassis until it clicks into place.



The module and slot are keyed. Do not force the module into the opening. If the module does not go in easily, realign the module and slide it into the chassis.

2. Repeat this step for the remaining DCPM module.

Step 9: Install fans into the chassis

Steps

To install the fan modules when replacing the chassis, you must perform a specific sequence of tasks.

1. Align the edges of the replacement fan module with the opening in the chassis, and then slide it into the chassis until it snaps into place.

When inserted into a live system, the amber Attention LED flashes four times when the fan module is successfully inserted into the chassis.

2. Repeat these steps for the remaining fan modules.
3. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.

Step 10: Install I/O modules

Steps

To install I/O modules, including the NVRAM/Flash Cache modules from the old chassis, follow the specific sequence of steps.

You must have the chassis installed so that you can install the I/O modules into the corresponding slots in the new chassis.

1. After the replacement chassis is installed in the rack or cabinet, install the I/O modules into their corresponding slots in the replacement chassis by gently sliding the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage, and then push the I/O cam latch all the way up to lock the module in place.
2. Recable the I/O module, as needed.
3. Repeat the preceding step for the remaining I/O modules that you set aside.



If the old chassis has blank I/O panels, move them to the replacement chassis at this time.

Step 11: Install the power supplies

Steps

Installing the power supplies when replacing a chassis involves installing the power supplies into the replacement chassis, and connecting to the power source.

1. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis until it locks into place.

The power supplies are keyed and can only be installed one way.



Do not use excessive force when sliding the power supply into the system. You can damage the connector.

2. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.



Only connect the power cable to the power supply. Do not connect the power cable to a power source at this time.

3. Repeat the preceding steps for any remaining power supplies.

Step 12: Install the controller

Steps

After you install the controller module and any other components into the new chassis, boot it.

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.



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

2. Recable the console to the controller module, and then reconnect the management port.

3. Connect the power supplies to different power sources, and then turn them on.
4. With the cam handle in the open position, slide the controller module into the chassis and firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle until it clicks into the locked position.



Do not use excessive force when sliding the controller module into the chassis; you might damage the connectors.

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

5. Repeat the preceding steps to install the second controller into the new chassis.
6. Boot each node to Maintenance mode:
 - a. As each node starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.



If you miss the prompt and the controller modules boot to ONTAP, enter `halt`, and then at the `LOADER` prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then repeat this step.

- b. From the boot menu, select the option for Maintenance mode.

Complete the restoration and replacement process - AFF A700

You must verify the HA state of the chassis and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

Step 1: Verify and set the HA state of the chassis

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

Steps

1. In Maintenance mode, from either controller module, display the HA state of the local controller module and chassis: `ha-config show`

The HA state should be the same for all components.

2. If the displayed system state for the chassis does not match your system configuration:
 - a. Set the HA state for the chassis: `ha-config modify chassis HA-state`

The value for `HA-state` can be one of the following:

- `ha`
- `mcc`
- `mcc-2n`
- `mccip`
- `non-ha`

- b. Confirm that the setting has changed: `ha-config show`
3. If you have not already done so, recable the rest of your system.
4. Exit Maintenance mode: `halt`

The LOADER prompt appears.

Step 2: Switch back aggregates in a two-node MetroCluster configuration

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the enabled state: `metrocluster node show`

```
cluster_B::> metrocluster node show

DR                               Configuration  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.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

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.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 3: Return the failed part to NetApp

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information.

Controller module

Overview of controller module replacement - AFF A700

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

- All drive shelves must be working properly.
- If your system has a V_StorageAttach license, you must refer to the additional required steps before performing this procedure.
- 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 your system is in a MetroCluster configuration, you must review the section [Choosing the correct recovery procedure](#) to determine whether you should use this procedure.

If this is the procedure you should use, note that the controller replacement procedure for a node in a four or eight node MetroCluster configuration is the same as that in an HA pair. No MetroCluster-specific steps are required because the failure is restricted to an HA pair and storage failover commands can be used to provide nondisruptive operation during the replacement.

- 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 drives or drive 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 module.
- 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.

Shut down the impaired controller - AFF 700

Shut down or take over the impaired controller using the appropriate procedure for your configuration.

Option 1: Most systems

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

About this task

- If you have a SAN system, you must have checked event messages (`cluster kernel-service show`) for the impaired controller SCSI blade. The `cluster kernel-service show` command (from `priv advanced` mode) displays the node name, [quorum status](#) of that node, availability status of that node, and operational status of that node.

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 cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see [Synchronize a node with the cluster](#).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=<# of hours>h
```

The following AutoSupport message suppresses automatic case creation for two hours:

```
cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Disable automatic giveback:

- a. Enter the following command from the console of the healthy controller:

```
storage failover modify -node impaired_node_name -auto-giveback false
```

- b. Enter `y` when you see the prompt *Do you want to disable auto-giveback?*

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.

If the impaired controller is displaying...	Then...
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

Option 2: Controller is in a two-node MetroCluster

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

About this task

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

Steps

- Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
- Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller...	Then...
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: <code>metrocluster switchover</code>
Has not automatically switched over, you attempted switchover with the <code>metrocluster switchover</code> command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

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

```
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.

```
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.

```
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.

```
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:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
    State: successful
Start Time: 7/29/2016 20:54:41
  End Time: 7/29/2016 20:54:42
  Errors: -
```

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

Replace the controller module hardware - AFF A700

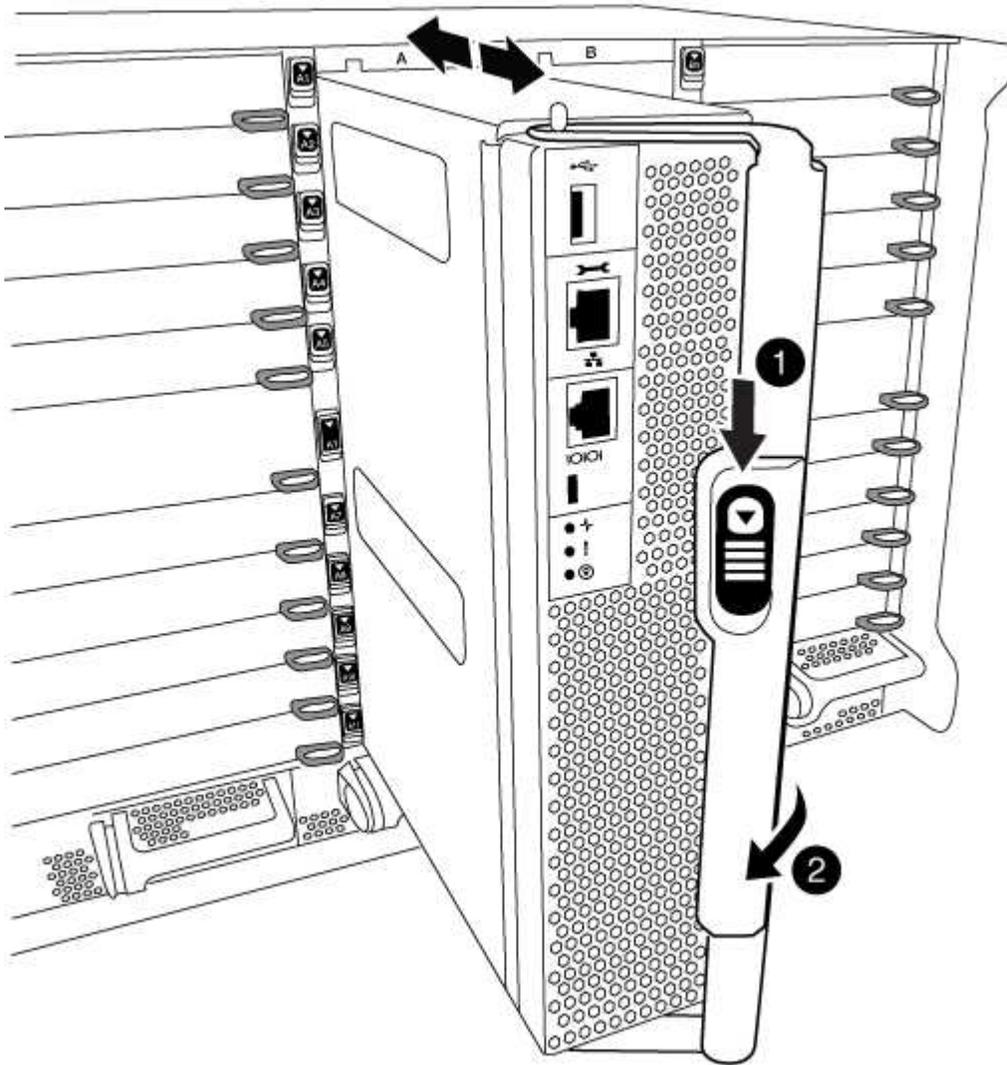
To replace the controller module hardware, you must remove the impaired node, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

Step 1: Remove the controller module

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

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

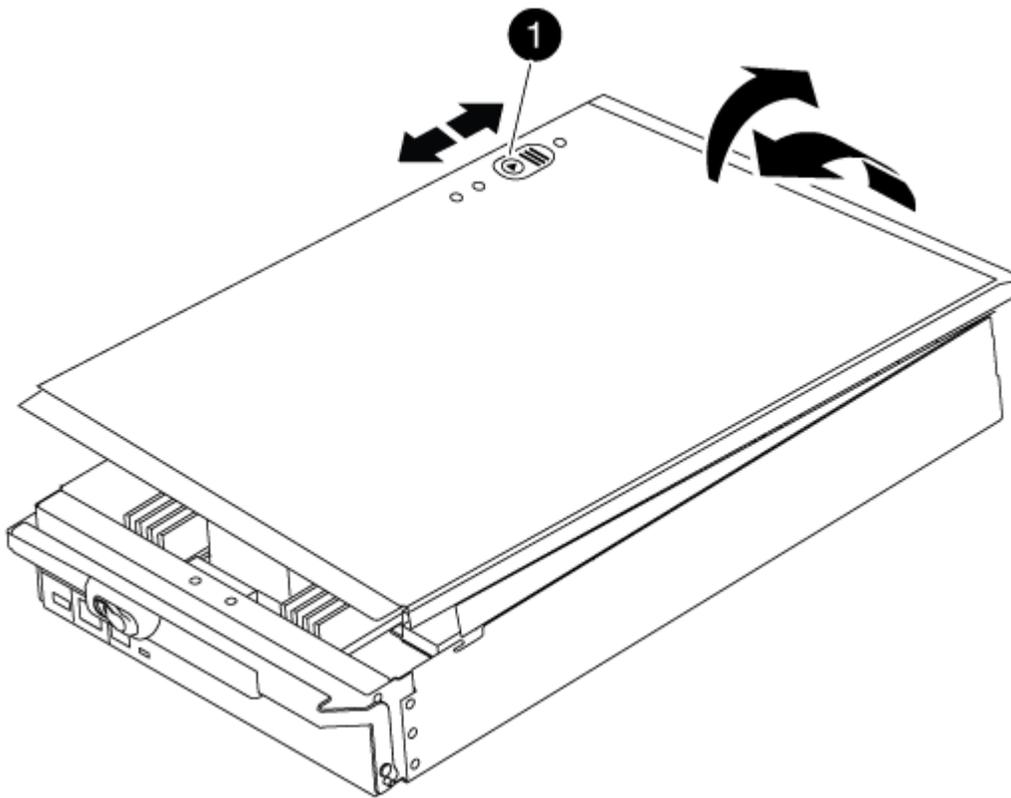


1	Cam handle release button
2	Cam handle

1. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

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

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



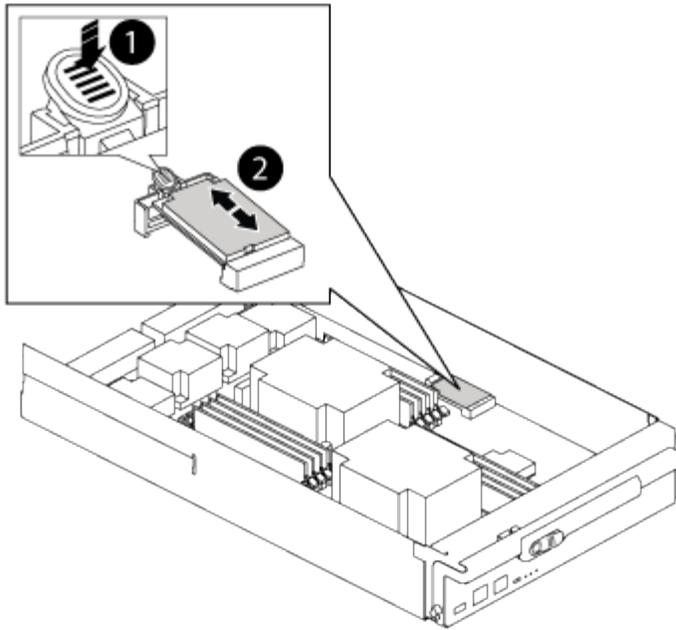
1	Controller module cover locking button
---	--

Step 2: Move the boot media

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

Steps

1. Lift the black air duct at the back of the controller module and then locate the boot media using the following illustration or the FRU map on the controller module:



1	Press release tab
2	Boot media

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.



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 reseal it into the socket.

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

Step 3: Move the system DIMMs

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

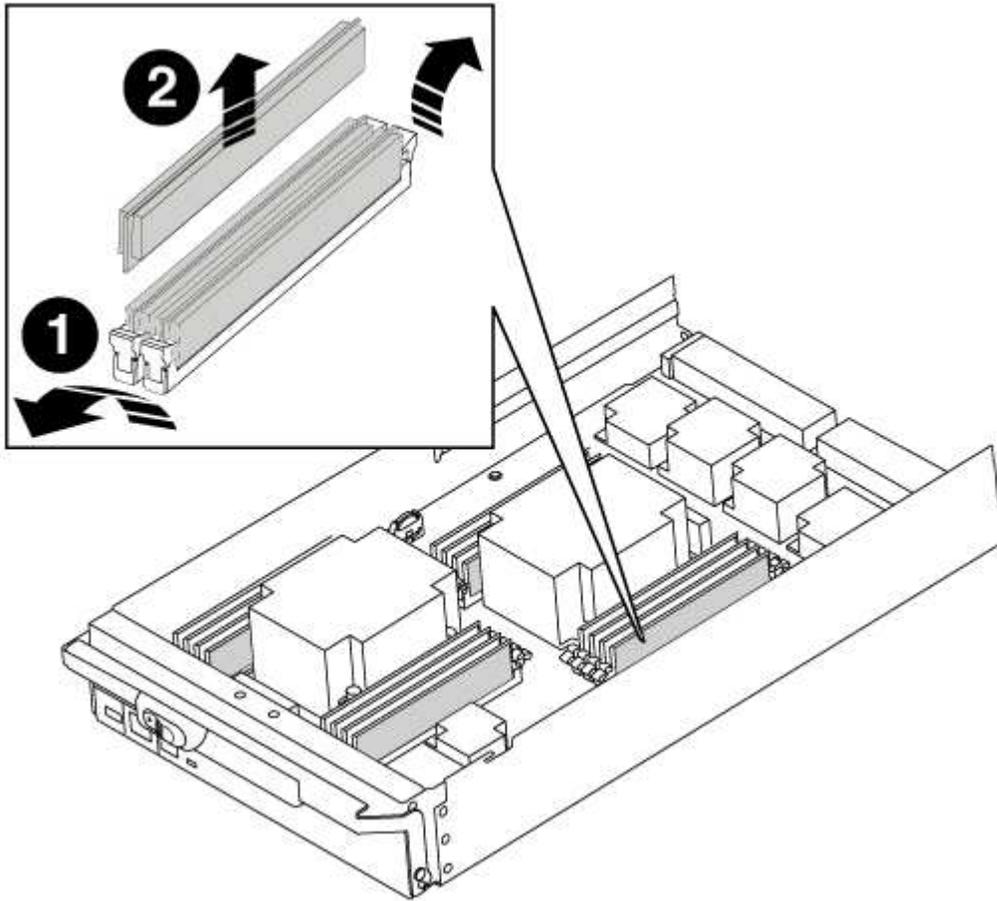
Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the DIMMs on your controller module.
3. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
4. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM,

and then slide the DIMM out of the slot.



Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.



1	DIMM ejector tabs
2	DIMM

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

6. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.



Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

7. Insert the DIMM squarely into the slot.

The DIMM fits tightly in the slot, but should go in easily. If not, realign the DIMM with the slot and reinsert it.



Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

8. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
9. Repeat these steps for the remaining DIMMs.

Step 4: Install the controller

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

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.



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

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.



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

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



You will connect the rest of the cables to the controller module later in this procedure.

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

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



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

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

- c. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
- d. Interrupt the boot process by pressing `Ctrl-C` when you see `Press Ctrl-C for Boot Menu`.
- e. Select the option to boot to Maintenance mode from the displayed menu.

Restore and verify the system configuration - AFF A700

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.

Step 1: Set and verify system time

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. If the *replacement* node is not at the LOADER prompt, halt the system to the LOADER prompt.
2. On the *healthy* node, check the system time: `cluster date show`

The date and time are based on the configured timezone.

3. At the LOADER prompt, check the date and time on the *replacement* node: `show date`

The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date mm/dd/yyyy`
5. If necessary, set the time in GMT on the replacement node: `set time hh:mm:ss`
6. At the LOADER prompt, confirm the date and time on the *replacement* node: `show date`

The date and time are given in GMT.

Step 2: Verify and set the controller's HA state

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`

The value for HA-state can be one of the following:

- `ha`
- `mcc`
- `mcc-2n`

- `mccip`
- `non-ha`
 - a. Confirm that the setting has changed: `ha-config show`

Recable the system and reassign disks - AFF A700

Continue the replacement procedure by recabling the storage and confirming disk reassignment.

Step 1: Recable the system

Verify the controller module's storage and network connections by using [Active IQ Config Advisor](#).

Steps

1. Download and install Config Advisor.
2. Enter the information for the target system, and then click Collect Data.
3. 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.
4. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

Step 2: Reassign disks

The procedure you use depends on your controller redundancy configuration.

Option 1: HA pair

=== Verify the system ID change on an HA system

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

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

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`

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`
```

Node	Partner	Takeover Possible	State Description
node1	node2	false	System ID changed on partner (Old: 151759706), In takeover
node2	node1	-	Waiting for giveback (HA mailboxes)

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 the `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. If your storage system has Storage or Volume Encryption configured, you must restore Storage or Volume Encryption functionality by using one of the following procedures, depending on whether you are using onboard or external key management:

- [Restore onboard key management encryption keys](#)
- [Restore external key management encryption keys](#)

6. Give back the node:

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



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.

7. Verify that the disks were assigned correctly: `storage disk show -ownership`

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`

Disk Aggregate Home  Owner  DR Home  Home ID      Owner ID      DR Home
ID Reserver  Pool
-----
-----
1.0.0  aggr0_1  node1  node1  -        1873775277  1873775277  -
1873775277 Pool10
1.0.1  aggr0_1  node1  node1  -        1873775277  1873775277  -
1873775277 Pool10
.
.
.
```

8. If the system is in a MetroCluster configuration, monitor the status of the node: `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 `metrocluster node show -fields node-systemid` command output displays

the old system ID until the MetroCluster configuration returns to a normal state.

9. 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.

[Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration](#)

10. If your system is in a MetroCluster configuration, verify that each node is configured: `metrocluster node show -fields configuration-state`

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

dr-group-id          cluster node          configuration-state
-----
-----
1 node1_siteA        node1mcc-001         configured
1 node1_siteA        node1mcc-002         configured
1 node1_siteB        node1mcc-003         configured
1 node1_siteB        node1mcc-004         configured

4 entries were displayed.
```

11. Verify that the expected volumes are present for each node: `vol show -node node-name`
12. If you disabled automatic takeover on reboot, enable it from the healthy node: `storage failover modify -node replacement-node-name -onreboot true`

Option 2: Two-node MetroCluster

=== Manually reassign 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``

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

```
dr-group-id cluster          node          node-systemid dr-
partner-systemid
-----
1          Cluster_A          Node_A_1          536872914
118073209
1          Cluster_B          Node_B_1          118073209
536872914
2 entries were displayed.
```

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

In this example, the new system ID is 118065481:

```
Local System ID: 118065481
...
...
```

4. Reassign disk ownership (for FAS 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 were assigned correctly: `disk show -a`

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
```

DISK	OWNER		POOL	SERIAL NUMBER	HOME
-----	-----		-----	-----	-----
disk_name (118065481)	system-1	(118065481)	Pool0	J8Y0TDZC	system-1
disk_name (118065481)	system-1	(118065481)	Pool0	J8Y09DXC	system-1
.					
.					
.					

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`

```

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

dr-group-id          cluster node          configuration-state
-----
-----
1 node1_siteA        node1mcc-001         configured
1 node1_siteA        node1mcc-002         configured
1 node1_siteB        node1mcc-003         configured
1 node1_siteB        node1mcc-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`

Complete system restoration - AFF A700

To complete the replacement procedure and restore your system to full operation, you must recable the storage, restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller. You must complete a series of tasks before restoring your system to full operation.

Step 1: Install 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.

Before you begin

If your system was initially running ONTAP 9.10.1 or later, use the procedure documented in [Post Motherboard Replacement Process to update Licensing on ONTAP platforms](#). If you are unsure of the initial ONTAP release for your system, see [NetApp Hardware Universe](#) for more information.

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.
- 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.



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

2. Install each license key: `system license add -license-code license-key, license-key...`
3. Remove the old licenses, if desired:
 - a. Check for unused licenses: `license clean-up -unused -simulate`
 - b. If the list looks correct, remove the unused licenses: `license clean-up -unused`

Step 2: Verifying LIFs and registering the serial number

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

Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`

If any LIFs are listed as false, revert them to their home ports: `network interface revert -vserver * -lif *`

2. Register the system serial number with NetApp Support.
 - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
 - If AutoSupport is not enabled, call [NetApp Support](#) to register the serial number.

3. Check the health of your cluster. See the [How to perform a cluster health check with a script in ONTAP KB](#) article for more information.
4. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.
5. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

Step 3: (MetroCluster only): Switching back aggregates in a two-node MetroCluster configuration

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the enabled state: `metrocluster node show`

```
cluster_B::> metrocluster node show

DR                               Configuration  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.
```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

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.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 4: Return the failed part to NetApp

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information.

Hot-swap a de-stage controller power module (DCPM) - AFF A700

To hot-swap a de-stage controller power module (DCPM), which contains the NVRAM10 battery, you must locate the failed DCPM module, remove it from the chassis, and install the replacement DCPM module.

You must have a replacement DCPM module in-hand before removing the failed module from the chassis and it must be replaced within five minutes of removal. Once the DCPM module is removed from the chassis, there is no shutdown protection for the controller module that owns the DCPM module, other than failover to the other controller module.

Step 1: Replace the DCPM module

To replace the DCPM module in your system, you must remove the failed DCPM module from the system and then replace it with a new DCPM module.

Steps

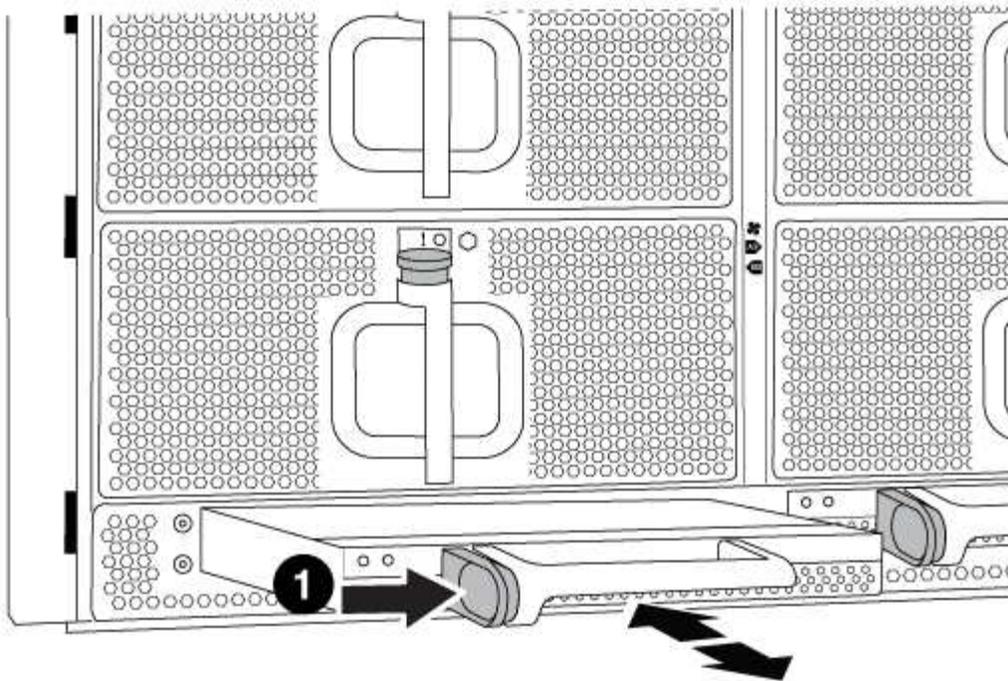
1. If you are not already grounded, properly ground yourself.
2. Remove the bezel on the front of the system and set it aside.
3. Locate the failed DCPM module in the front of the system by looking for the Attention LED on the module.

The LED will be steady amber if the module is faulty.



The DCPM module must be replaced in the chassis within five minutes of removal or the associated controller will shut down.

4. Press the orange locking button on the module handle, and then slide the DCPM module out of the chassis.



1	DCPM module orange locking button
----------	-----------------------------------

5. Align the end of the DCPM module with the chassis opening, and then gently slide it into the chassis until it clicks into place.



The module and slot are keyed. Do not force the module into the opening. If the module does not go in easily, realign the module and slide it into the chassis.

The DCPM module LED lights when the module is fully seated into the chassis.

Step 2: Dispose of batteries

You must dispose of batteries according to the local regulations regarding battery recycling or disposal. If you cannot properly dispose of batteries, you must return the batteries to NetApp, as described in the RMA instructions that are shipped with the kit.

https://library.netapp.com/ecm/ecm_download_file/ECMP12475945

Step 3: Return the failed part to NetApp

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information.

Replace a DIMM - AFF A700

You must replace a DIMM in the controller when your storage system encounters errors such as, excessive CECC (Correctable Error Correction Codes) errors that are based on

Health Monitor alerts or uncorrectable ECC errors, typically caused by a single DIMM failure preventing the storage system from booting ONTAP.

All other components in the system must be functioning properly; if not, you must contact technical support.

You must replace the failed component with a replacement FRU component you received from your provider.

Step 1: Shut down the impaired controller

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

Option 1: Most configurations

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

About this task

- If you have a SAN system, you must have checked event messages (`cluster kernel-service show`) for the impaired controller SCSI blade. The `cluster kernel-service show` command (from `priv advanced` mode) displays the node name, [quorum status](#) of that node, availability status of that node, and operational status of that node.

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 cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see [Synchronize a node with the cluster](#).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=<# of hours>h
```

The following AutoSupport message suppresses automatic case creation for two hours:

```
cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Disable automatic giveback:

- a. Enter the following command from the console of the healthy controller:

```
storage failover modify -node impaired_node_name -auto-giveback false
```

- b. Enter `y` when you see the prompt *Do you want to disable auto-giveback?*

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.

If the impaired controller is displaying...	Then...
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

Option 2: Controller is in a two-node MetroCluster

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

About this task

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

Steps

- Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
- Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller...	Then...
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: <code>metrocluster switchover</code>
Has not automatically switched over, you attempted switchover with the <code>metrocluster switchover</code> command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

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

```
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.

```
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.

```
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.

```
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:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
    State: successful
Start Time: 7/29/2016 20:54:41
  End Time: 7/29/2016 20:54:42
  Errors: -
```

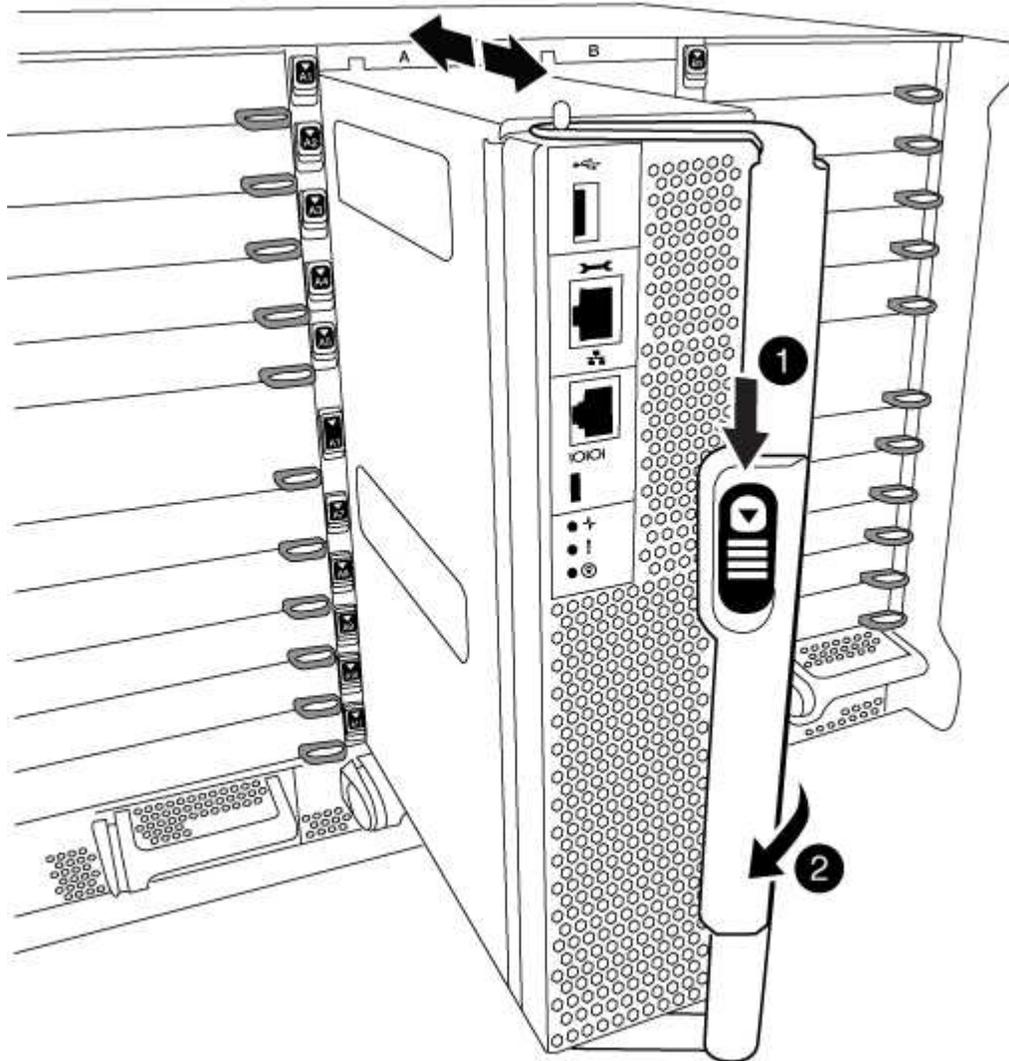
8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

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

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

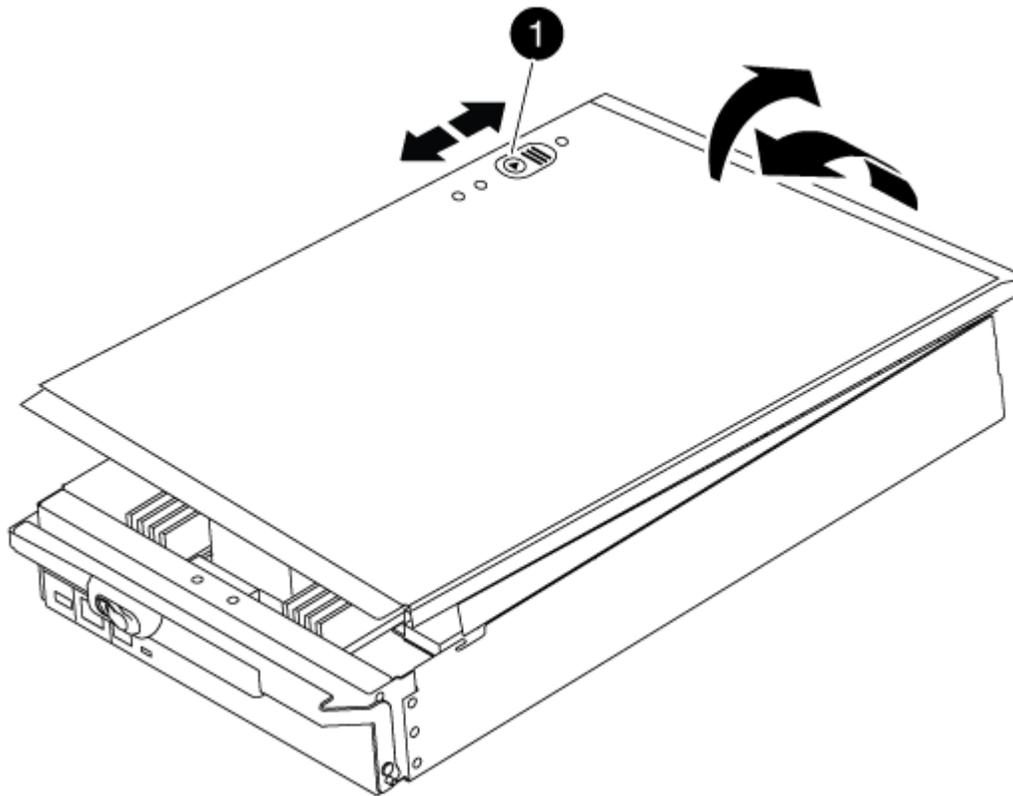


1	Cam handle release button
2	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

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

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



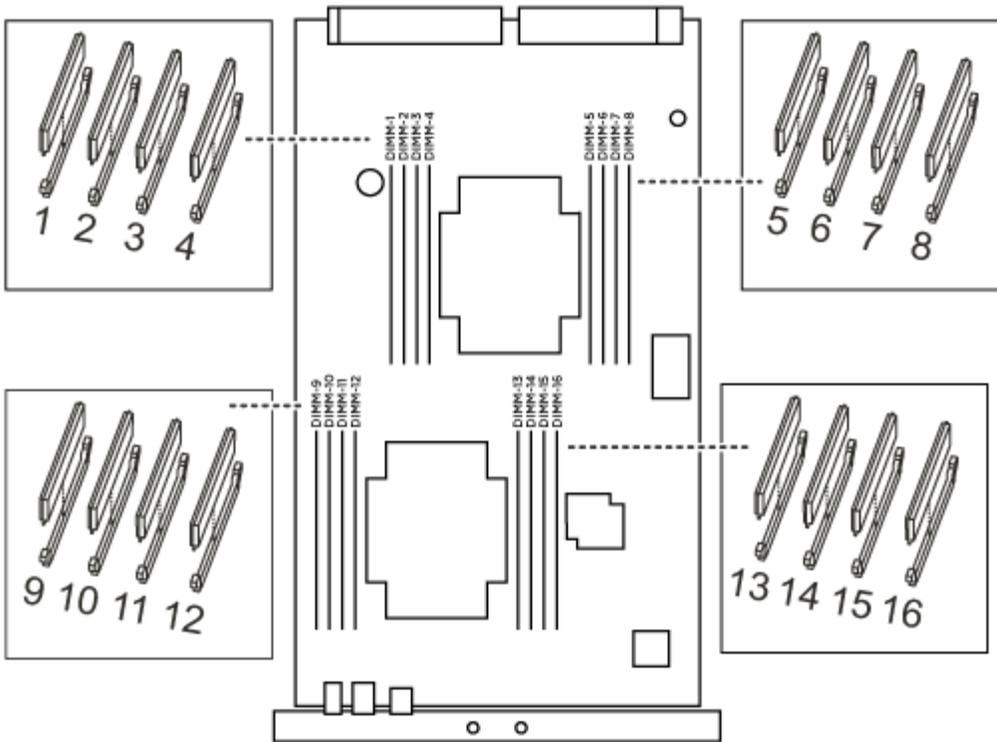
1	Controller module cover locking button
----------	--

Step 3: Replace the DIMMs

To replace the DIMMs, locate them inside the controller and follow the specific sequence of steps.

Steps

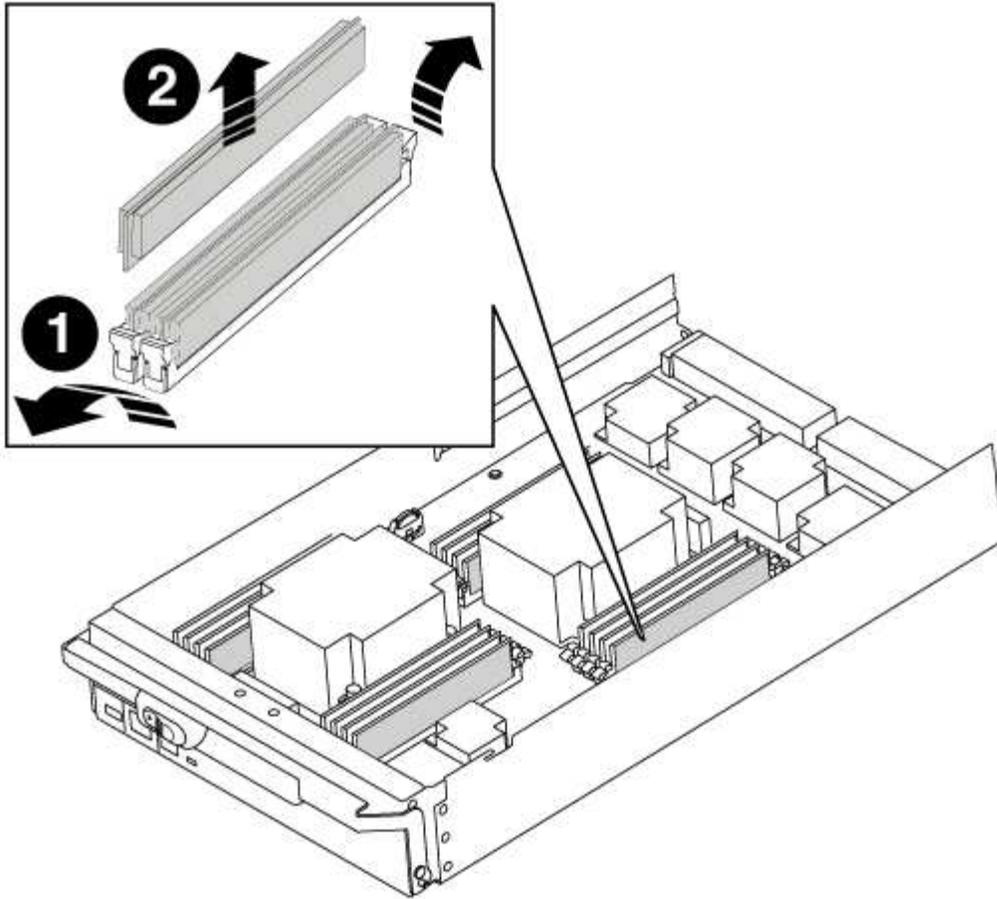
1. If you are not already grounded, properly ground yourself.
2. Locate the DIMMs on your controller module.



1. 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.



Carefully hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.



1	DIMM ejector tabs
2	DIMM

2. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

The notch among the pins on the DIMM should line up with the tab in the socket.

3. 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.



Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

4. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
5. Close the controller module cover.

Step 4: Install the controller

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

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.

Steps

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.



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

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



You will connect the rest of the cables to the controller module later in this procedure.

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

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



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

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

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

Step 5: Switch back aggregates in a two-node MetroCluster configuration

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the `enabled state`: `metrocluster node show`

```

cluster_B::> metrocluster node show

DR
Group Cluster Node          Configuration  DR
-----
-----
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.

```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

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.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information.

Swap out a fan - AFF A700

To swap out a fan module without interrupting service, you must perform a specific sequence of tasks.



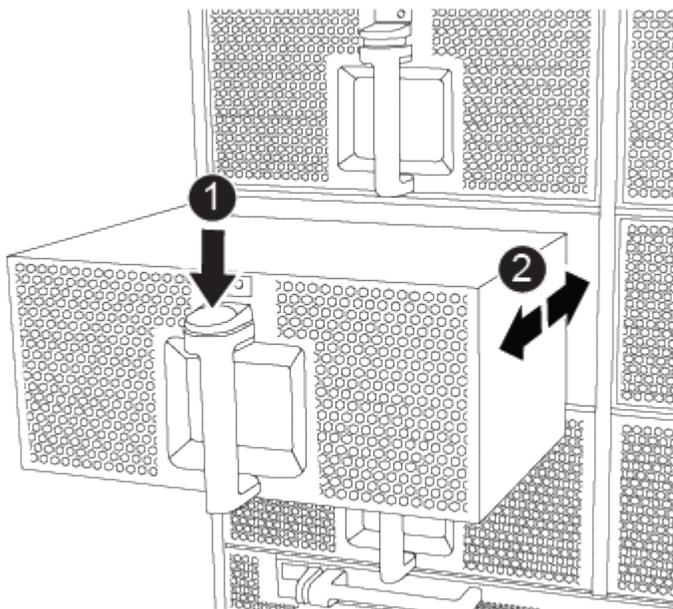
You must replace the fan module within two minutes of removing it from the chassis. System airflow is disrupted and the controller module or modules shut down after two minutes to avoid overheating.

Steps

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Identify the fan module that you must replace by checking the console error messages and looking at the Attention LED on each fan module.
4. Press the orange button on the fan module and pull the fan module straight out of the chassis, making sure that you support it with your free hand.



The fan modules are short. Always support the bottom of the fan module with your free hand so that it does not suddenly drop free from the chassis and injure you.



1

Orange release button

5. Set the fan module aside.

6. Align the edges of the replacement fan module with the opening in the chassis, and then slide it into the chassis until it snaps into place.

When inserted into a live system, the amber Attention LED flashes four times when the fan module is successfully inserted into the chassis.

7. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.
8. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information.

Replace an I/O module - AFF A700 and FAS9000

To replace an I/O module, you must perform a specific sequence of tasks.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

Step 1: Shut down the impaired controller

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

Option 1: Most configurations

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

About this task

- If you have a SAN system, you must have checked event messages (`cluster kernel-service show`) for the impaired controller SCSI blade. The `cluster kernel-service show` command (from `priv advanced` mode) displays the node name, [quorum status](#) of that node, availability status of that node, and operational status of that node.

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 cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see [Synchronize a node with the cluster](#).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=<# of hours>h
```

The following AutoSupport message suppresses automatic case creation for two hours:

```
cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Disable automatic giveback:

- a. Enter the following command from the console of the healthy controller:

```
storage failover modify -node impaired_node_name -auto-giveback false
```

- b. Enter `y` when you see the prompt *Do you want to disable auto-giveback?*

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.

If the impaired controller is displaying...	Then...
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

Option 2: Controller is in a two-node MetroCluster

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

About this task

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

Steps

- Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
- Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller...	Then...
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: <code>metrocluster switchover</code>
Has not automatically switched over, you attempted switchover with the <code>metrocluster switchover</code> command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

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

```
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.

```
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.

```
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.

```
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:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
    State: successful
Start Time: 7/29/2016 20:54:41
  End Time: 7/29/2016 20:54:42
  Errors: -
```

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

Step 2: Replace I/O modules

To replace an I/O module, locate it within the chassis and follow the specific sequence of steps.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug any cabling associated with the target I/O module.

Make sure that you label the cables so that you know where they came from.

3. Remove the target I/O module from the chassis:

- a. Depress the lettered and numbered cam button.

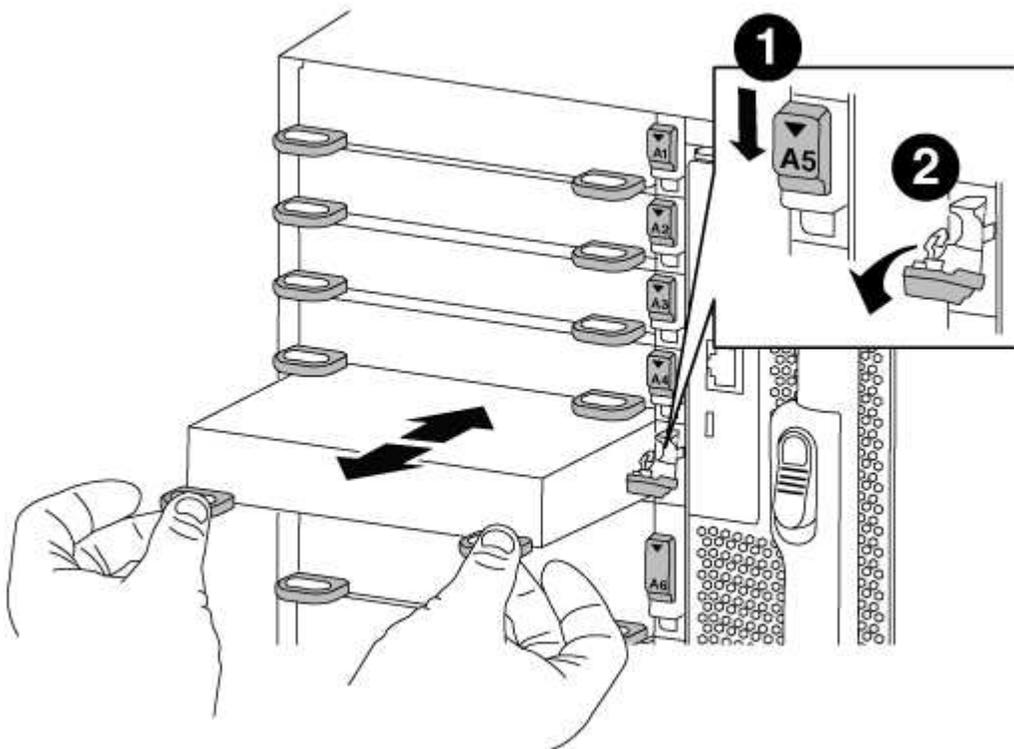
The cam button moves away from the chassis.

- b. Rotate the cam latch down until it is in a horizontal position.

The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

- c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

Make sure that you keep track of which slot the I/O module was in.



1	Lettered and numbered I/O cam latch
2	I/O cam latch completely unlocked

4. Set the I/O module aside.
5. Install the replacement I/O module into the chassis by gently sliding the I/O 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.
6. Recable the I/O module, as needed.

Step 3: Reboot the controller after I/O module replacement

After you replace an I/O module, you must reboot the controller module.



If the new I/O module is not the same model as the failed module, you must first reboot the BMC.

Steps

1. Reboot the BMC if the replacement module is not the same model as the old module:
 - a. From the LOADER prompt, change to advanced privilege mode: `priv set advanced`
 - b. Reboot the BMC: `sp reboot`
2. From the LOADER prompt, reboot the node: `bye`



This reinitializes the PCIe cards and other components and reboots the node.

3. If your system is configured to support 10 GbE cluster interconnect and data connections on 40 GbE NICs or onboard ports, convert these ports to 10 GbE connections by using the `nicadmin convert` command from Maintenance mode.



Be sure to exit Maintenance mode after completing the conversion.

4. Return the node to normal operation: `storage failover giveback -ofnode impaired_node_name`
5. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`



If your system is in a two-node MetroCluster configuration, you must switch back the aggregates as described in the next step.

Step 4: Switch back aggregates in a two-node MetroCluster configuration

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the enabled state: `metrocluster node show`

```

cluster_B::> metrocluster node show

DR
Group Cluster Node          Configuration  DR
-----
-----
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.

```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

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.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 5: Return the failed part to NetApp

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information.

Replace an LED USB module - AFF A700

You can replace an LED USB module without interrupting service.

The FAS9000 or AFF A700 LED USB module provides connectivity to console ports and system status. Replacement of this module does not require tools.

Steps

1. Remove the old LED USB module:



- a. With the bezel removed, locate the LED USB module at the front of the chassis, on the bottom left side.
- b. Slide the latch to partially eject the module.
- c. Pull the module out of the bay to disconnect it from the midplane. Do not leave the slot empty.

2. Install the new LED USB module:



- a. Align the module to the bay with the notch in the corner of the module positioned near the slider latch on the chassis. The bay will prevent you from installing the module upside down.

- b. Push the module into the bay until it is fully seated flush with the chassis.

There is an audible click when the module is secure and connected to the midplane.

Return the failed part to NetApp

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information.

Replace the NVRAM module or NVRAM DIMMs - AFF A700

The NVRAM module consists of the NVRAM10 and DIMMs and up to two NVMe SSD Flash Cache modules (Flash Cache 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 Flash Cache module or modules from the NVRAM module, move the DIMMs to the replacement module, reinstall the Flash Cache 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.
- 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.

Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using one of the following options.

Option 1: Most systems

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

About this task

- If you have a SAN system, you must have checked event messages (`cluster kernel-service show`) for the impaired controller SCSI blade. The `cluster kernel-service show` command (from `priv advanced` mode) displays the node name, [quorum status](#) of that node, availability status of that node, and operational status of that node.

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 cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see [Synchronize a node with the cluster](#).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=<# of hours>h
```

The following AutoSupport message suppresses automatic case creation for two hours:

```
cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Disable automatic giveback:

- a. Enter the following command from the console of the healthy controller:

```
storage failover modify -node impaired_node_name -auto-giveback false
```

- b. Enter `y` when you see the prompt *Do you want to disable auto-giveback?*

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.

If the impaired controller is displaying...	Then...
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

Option 2: Controller is in a Two-node MetroCluster

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

About this task

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

Steps

- Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
- Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller...	Then...
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: <code>metrocluster switchover</code>
Has not automatically switched over, you attempted switchover with the <code>metrocluster switchover</code> command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

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

```
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.

```
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.

```
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.

```
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:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
    State: successful
Start Time: 7/29/2016 20:54:41
  End Time: 7/29/2016 20:54:42
  Errors: -
```

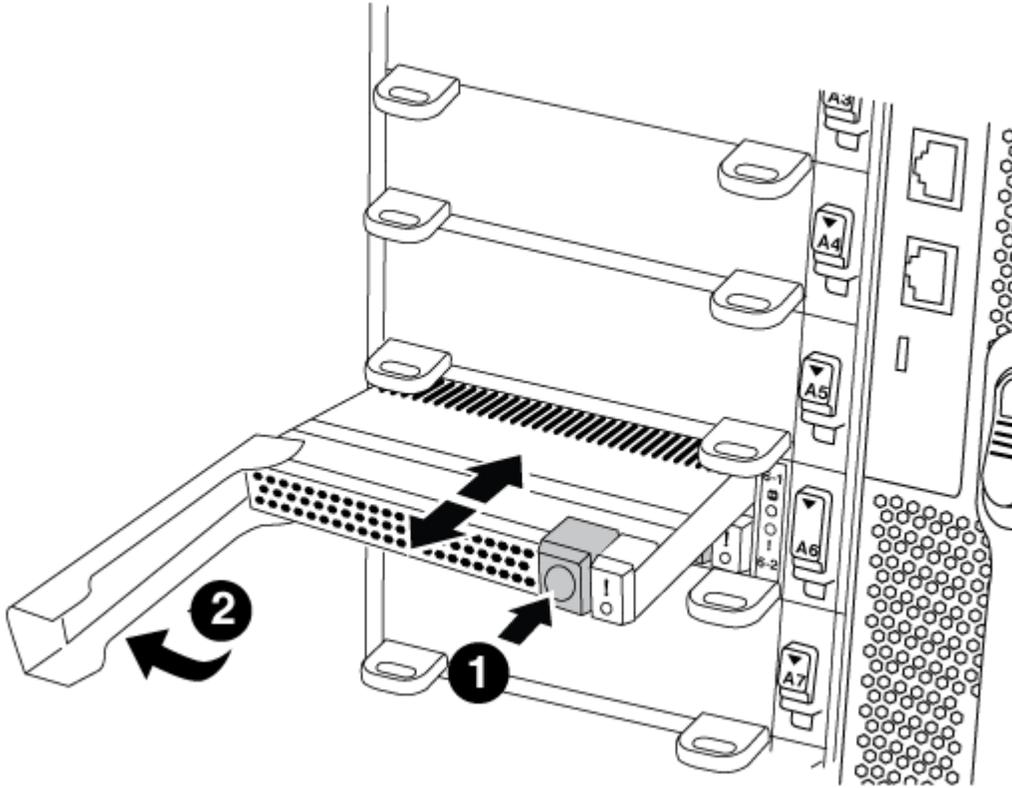
8. On the impaired controller module, disconnect the power supplies.

Step 2: Replace 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 Flash Cache module from the old NVRAM module to the new NVRAM module:



1	Orange release button (gray on empty Flash Cache modules)
2	Flash Cache cam handle

- a. Press the orange button on the front of the Flash Cache module.



The release button on empty Flash Cache modules is gray.

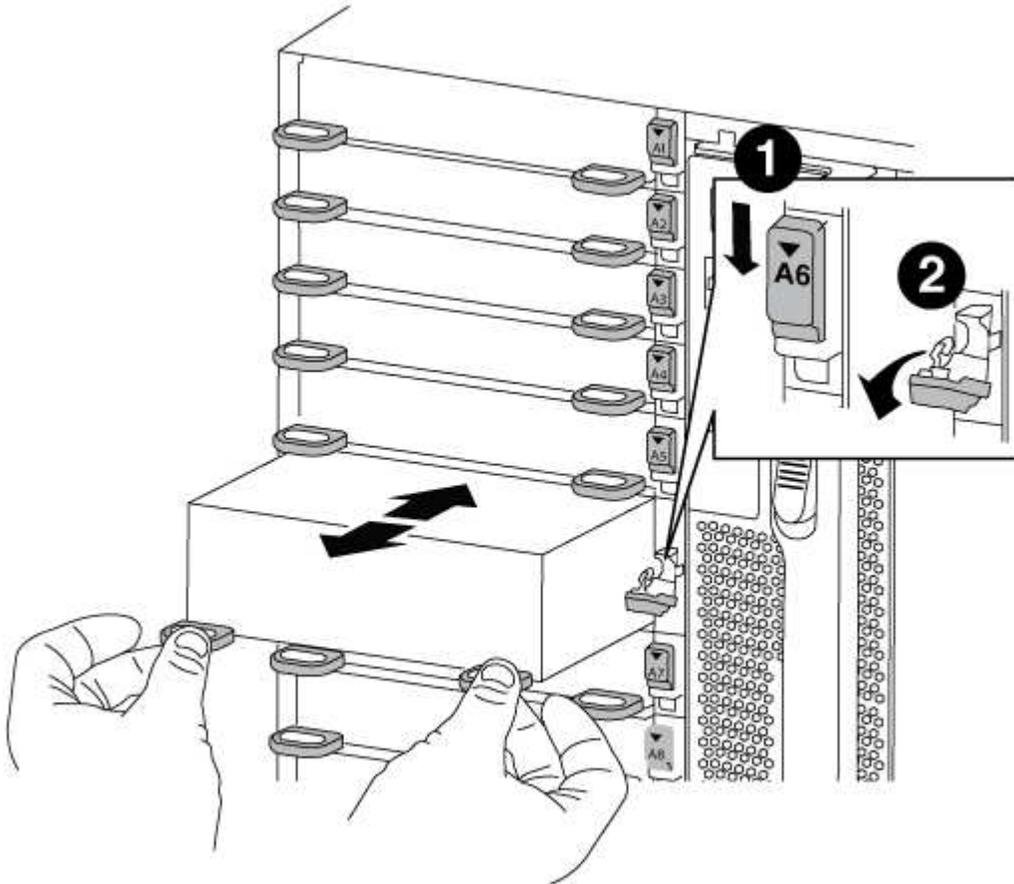
- b. Swing the cam handle out until the module begins to slide out of the old NVRAM module.
 - c. Grasp the module cam handle and slide it out of the NVRAM module and insert it into the front of the new NVRAM module.
 - d. Gently push the Flash Cache module all the way into the NVRAM module, and then swing the cam handle 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.

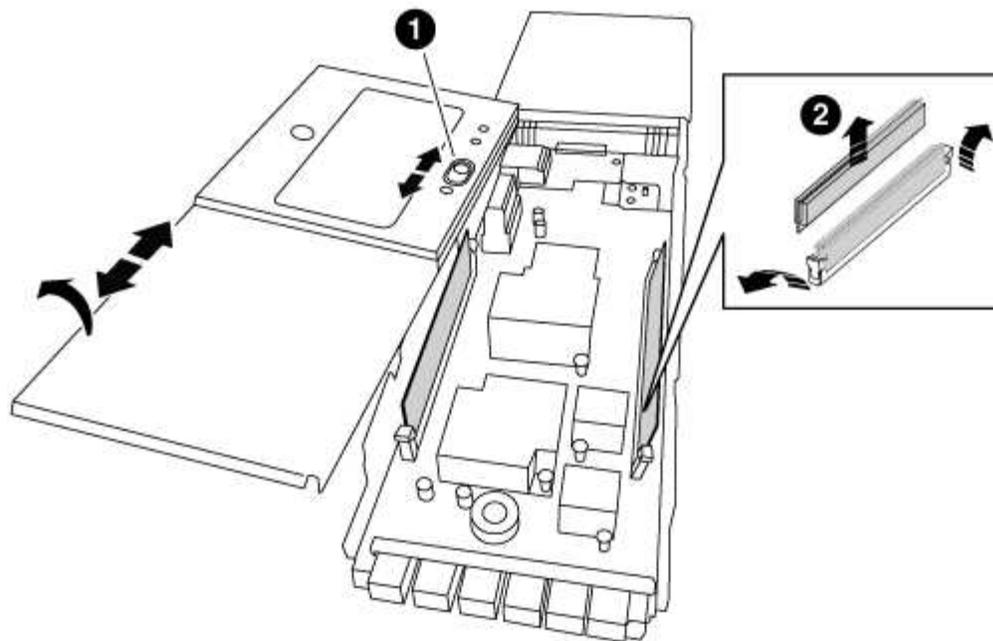
The NVRAM module disengages from the chassis and moves out a few inches.

- 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

- 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 down the blue button, slide the lid off the NVRAM module.



1	Cover locking button
2	DIMM and DIMM ejector tabs

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.

Step 3: Replace 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.

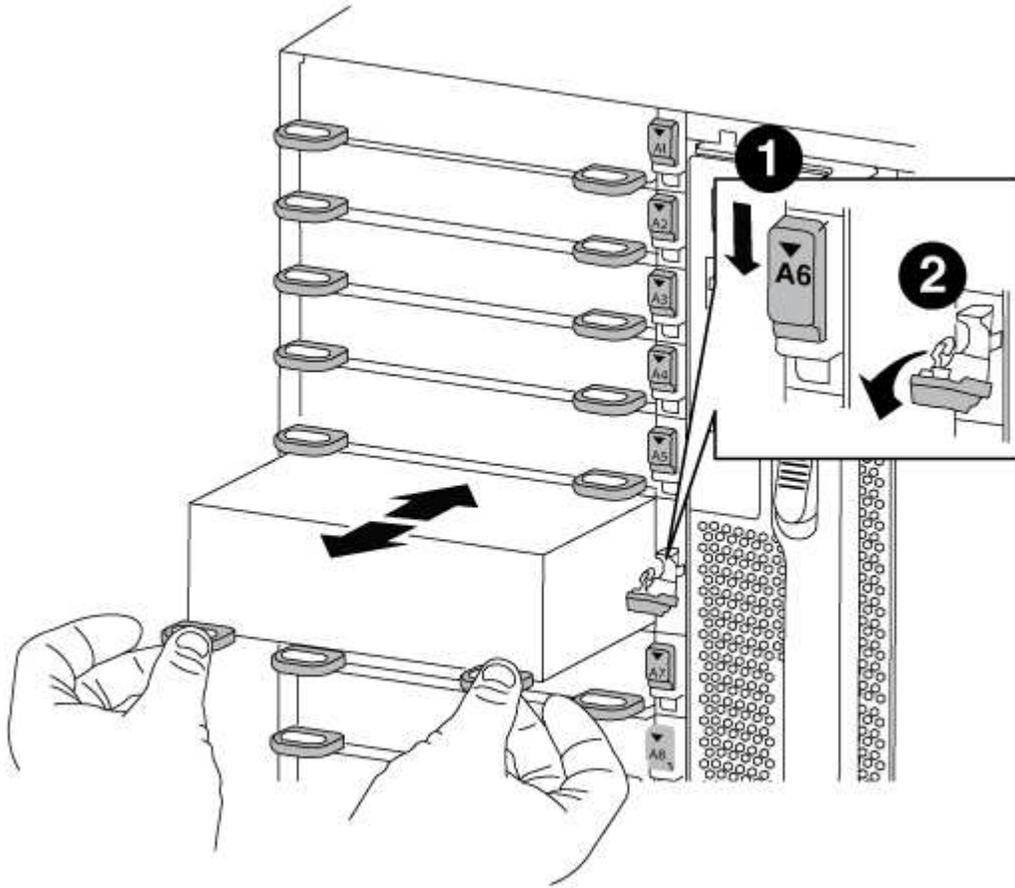
Steps

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.

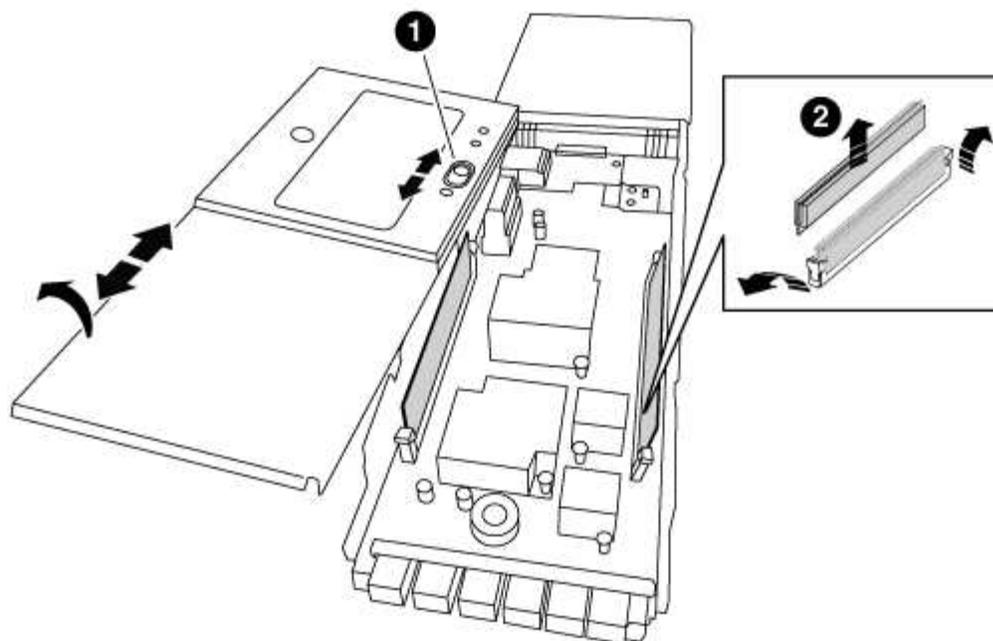
The NVRAM module disengages from the chassis and moves out a few inches.

- 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 down the blue button, slide the lid off the NVRAM module.



1	Cover locking button
2	DIMM and DIMM ejector tabs

4. Locate the DIMM to be replaced inside the NVRAM module, and then remove it by pressing down on the DIMM locking tabs and lifting the DIMM out of the socket.
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.

Step 4: Reboot the controller after FRU replacement

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

Step

1. To boot ONTAP from the LOADER prompt, enter `bye`.

Step 5: Reassign disks

Depending on whether you have an HA pair or two-node MetroCluster configuration, you must either verify the reassignment of disks to the new controller module or manually reassign the disks.

Select one of the following options for instructions on how to reassign disks to the new controller.

Option 1: Verify ID (HA pair)

Verify 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.



Disk reassignment is only needed when replacing the NVRAM module and does not apply to NVRAM DIMM replacement.

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 bye
```

The node will reboot, if autoboot is set.

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`

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`
```

Node	Partner	Takeover Possible	State Description
node1	node2	false	System ID changed on partner (Old: 151759706), In takeover
node2	node1	-	Waiting for giveback (HA mailboxes)

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 the `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: `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`.



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. Verify that the disks were assigned correctly: `storage disk show -ownership`

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`

Disk  Aggregate Home  Owner  DR Home  Home ID      Owner ID      DR Home
ID Reserver  Pool
-----
-----
-----
1.0.0  aggr0_1  node1  node1  -        1873775277  1873775277  -
1873775277 Pool10
1.0.1  aggr0_1  node1  node1  -        1873775277  1873775277  -
1873775277 Pool10
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the node: `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 `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

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.

[Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration](#)

9. If your system is in a MetroCluster configuration, verify that each node is configured: `metrocluster node show -fields configuration-state`

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

dr-group-id          cluster node          configuration-state
-----
-----
1 node1_siteA        node1mcc-001         configured
1 node1_siteA        node1mcc-002         configured
1 node1_siteB        node1mcc-003         configured
1 node1_siteB        node1mcc-004         configured

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`

Option 2: Reassign ID (MetroCluster config)

Reassign the system ID 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``

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

```
dr-group-id cluster          node          node-systemid dr-
partner-systemid
-----
1          Cluster_A          Node_A_1          536872914
118073209
1          Cluster_B          Node_B_1          118073209
536872914
2 entries were displayed.
```

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

In this example, the new system ID is 118065481:

```
Local System ID: 118065481
...
...
```

4. Reassign disk ownership (for FAS 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 were assigned correctly: `disk show -a`

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
```

DISK	OWNER		POOL	SERIAL NUMBER	HOME
-----	-----		-----	-----	-----
disk_name (118065481)	system-1	(118065481)	Pool0	J8Y0TDZC	system-1
disk_name (118065481)	system-1	(118065481)	Pool0	J8Y09DXC	system-1
.					
.					
.					

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`

```

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

dr-group-id          cluster node          configuration-state
-----
-----
1 node1_siteA        node1mcc-001         configured
1 node1_siteA        node1mcc-002         configured
1 node1_siteB        node1mcc-003         configured
1 node1_siteB        node1mcc-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`

Step 6: Return the failed part to NetApp

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information.

Hot-swap a power supply - AFF A700

Swapping out a power supply involves turning off, disconnecting, and removing the old power supply and installing, connecting, and turning on the replacement power supply.

All other components in the system must be functioning properly; if not, you must contact technical support.

- The power supplies are redundant and hot-swappable. You do not have to shut down the controller to replace a PSU.
- This procedure is written for replacing one power supply at a time.



It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

- The number of power supplies in the system depends on the model.
- Power supplies are auto-ranging.



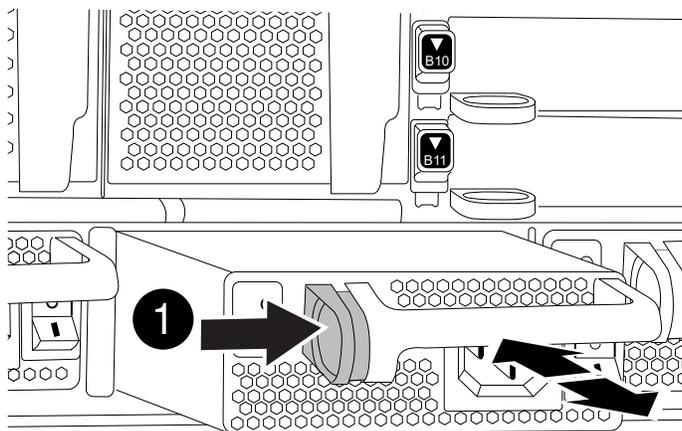
Do not mix PSUs with different efficiency ratings. Always replace like for like.

Steps

1. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
2. If you are not already grounded, properly ground yourself.
3. Turn off the power supply and disconnect the power cables:
 - a. Turn off the power switch on the power supply.
 - b. Open the power cable retainer, and then unplug the power cable from the power supply.
 - c. Unplug the power cable from the power source.
4. Press and hold the orange button on the power supply handle, and then pull the power supply out of the chassis.



When removing a power supply, always use two hands to support its weight.



1	Locking button
----------	----------------

5. Make sure that the on/off switch of the new power supply is in the Off position.
6. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis until it locks into place.

The power supplies are keyed and can only be installed one way.



Do not use excessive force when sliding the power supply into the system. You can damage the connector.

7. Reconnect the power supply cabling:
 - a. Reconnect the power cable to the power supply and the power source.
 - b. Secure the power cable to the power supply using the power cable retainer.

Once power is restored to the power supply, the status LED should be green.

8. Turn on the power to the new power supply, and then verify the operation of the power supply activity LEDs.

The green power LED lights when the PSU is fully inserted into the chassis and the amber attention LED flashes initially, but turns off after a few moments.

9. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information.

Replace the real-time clock battery - AFF 700

You replace the real-time clock (RTC) battery in the controller module so that your system's services and applications that depend on accurate time synchronization continue to function.

- You can use this procedure with all versions of ONTAP supported by your system
- All other components in the system must be functioning properly; if not, you must contact technical support.

You must use an approved RTC battery.

Step 1: Shut down the impaired controller

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

Option 1: Most configurations

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

About this task

- If you have a SAN system, you must have checked event messages (`cluster kernel-service show`) for the impaired controller SCSI blade. The `cluster kernel-service show` command (from `priv advanced` mode) displays the node name, [quorum status](#) of that node, availability status of that node, and operational status of that node.

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 cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see [Synchronize a node with the cluster](#).

Steps

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=<# of hours>h
```

The following AutoSupport message suppresses automatic case creation for two hours:

```
cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Disable automatic giveback:

- a. Enter the following command from the console of the healthy controller:

```
storage failover modify -node impaired_node_name -auto-giveback false
```

- b. Enter `y` when you see the prompt *Do you want to disable auto-giveback?*

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.

If the impaired controller is displaying...	Then...
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

Option 2: Controller is in a two-node MetroCluster

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

About this task

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

Steps

- Check the MetroCluster status to determine whether the impaired controller has automatically switched over to the healthy controller: `metrocluster show`
- Depending on whether an automatic switchover has occurred, proceed according to the following table:

If the impaired controller...	Then...
Has automatically switched over	Proceed to the next step.
Has not automatically switched over	Perform a planned switchover operation from the healthy controller: <code>metrocluster switchover</code>
Has not automatically switched over, you attempted switchover with the <code>metrocluster switchover</code> command, and the switchover was vetoed	Review the veto messages and, if possible, resolve the issue and try again. If you are unable to resolve the issue, contact technical support.

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

```
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.

```
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.

```
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.

```
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:

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
    State: successful
Start Time: 7/29/2016 20:54:41
  End Time: 7/29/2016 20:54:42
  Errors: -
```

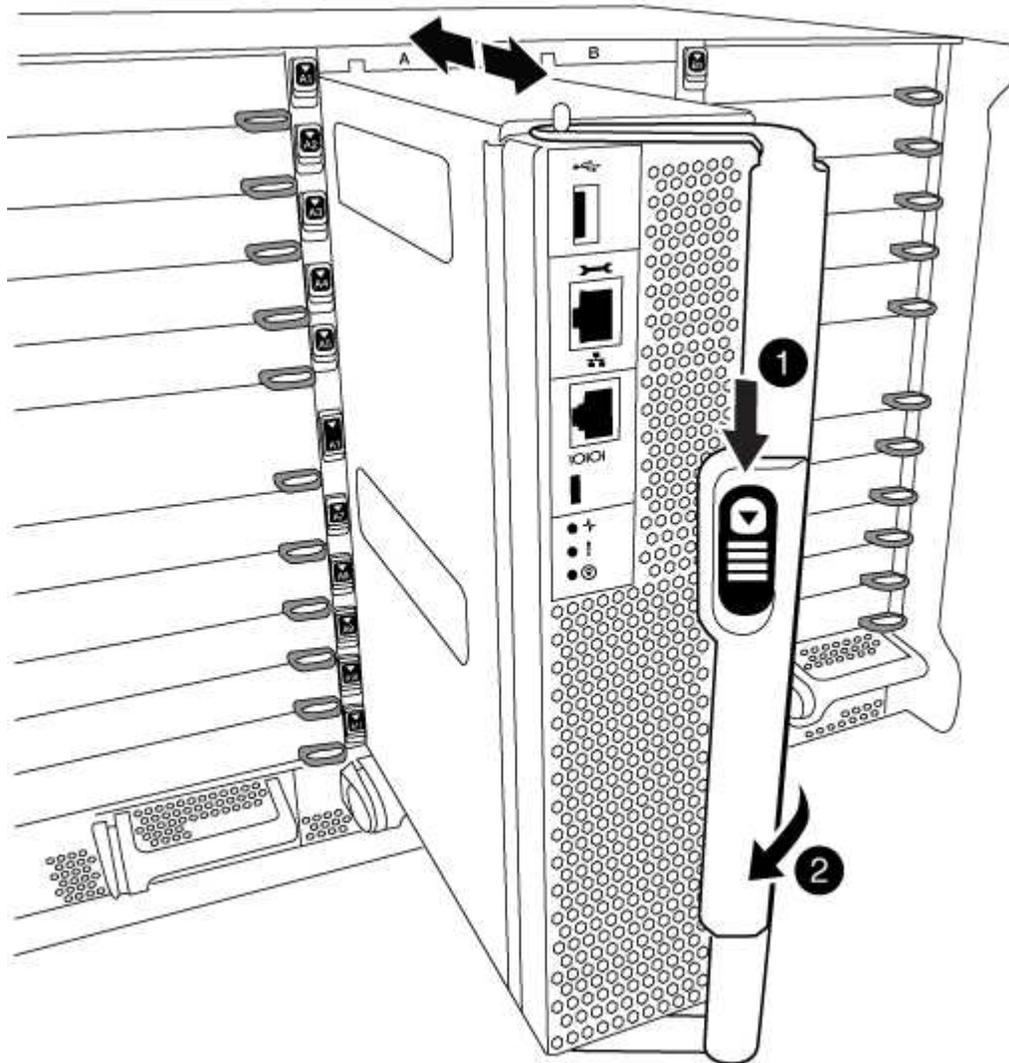
8. On the impaired controller module, disconnect the power supplies.

Step 2: Remove the controller module

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

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the orange button on the cam handle downward until it unlocks.

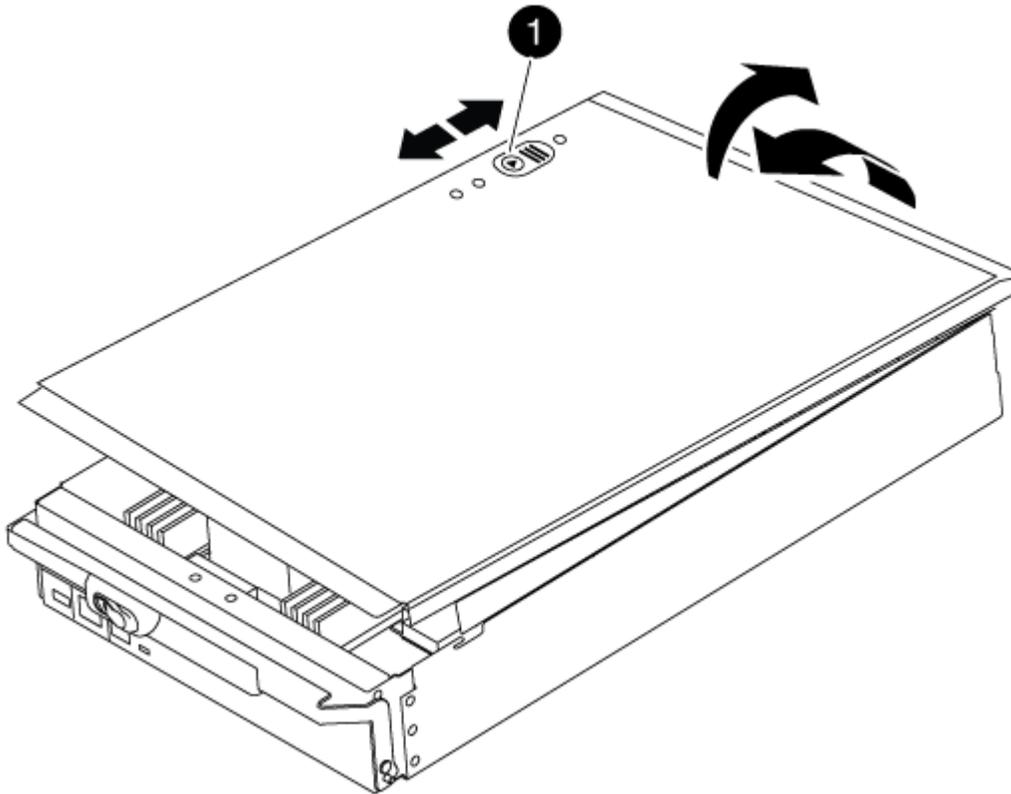


1	Cam handle release button
2	Cam handle

4. Rotate the cam handle so that it completely disengages the controller module from the chassis, and then slide the controller module out of the chassis.

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

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



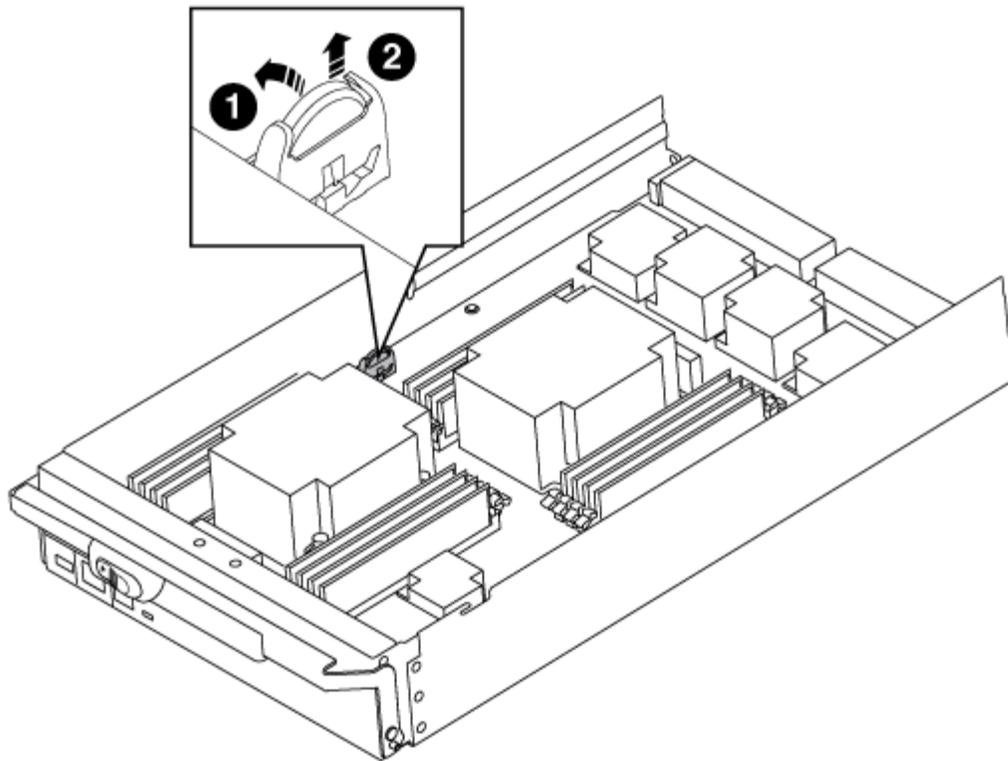
1	Controller module cover locking button
----------	--

Step 3: Replace the RTC battery

To replace the RTC battery, you must locate the failed battery in the controller module, remove it from the holder, and then install the replacement battery in the holder.

Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the RTC battery.



1	RTC battery
2	RTC battery housing

3. Gently push the battery away from the holder, rotate it away from the holder, and then lift it out of the holder.



Note the polarity of the battery as you remove it from the holder. The battery is marked with a plus sign and must be positioned in the holder correctly. A plus sign near the holder tells you how the battery should be positioned.

4. Remove the replacement battery from the antistatic shipping bag.
5. Locate the empty battery holder in the controller module.
6. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
7. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.
8. Reinstall the controller module cover.

Step 4: Reinstall the controller module and set time/date

After you replace a component within the controller module, you must reinstall the controller module in the system chassis, reset the time and date on the controller, and then boot it.

Steps

1. If you have not already done so, close the air duct or controller module cover.
2. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.

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

3. Recable the system, as needed.

If you removed the media converters (QSFPs or SFPs), remember to reinstall them if you are using fiber optic cables.

4. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:

- 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.



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, and then turn on the power to start the boot process.
 - e. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
 - a. Check the date and time on the healthy node with the `show date` command.
 - b. At the LOADER prompt on the target node, check the time and date.
 - c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
 - d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
 - e. Confirm the date and time on the target node.
 7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the node reboot.
 8. Return the node to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
 9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

Step 5: Switch back aggregates in a two-node MetroCluster configuration

This task only applies to two-node MetroCluster configurations.

Steps

1. Verify that all nodes are in the enabled state: `metrocluster node show`

```

cluster_B::> metrocluster node show

DR
Group Cluster Node          Configuration  DR
-----
-----
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.

```

2. Verify that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations were completed successfully: `metrocluster check lif show`
4. Perform the switchback by using the `metrocluster switchback` command from any node in the surviving cluster.
5. Verify that the switchback operation has completed: `metrocluster show`

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.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 6: Return the failed part to NetApp

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return and Replacements](#) page for further information.

X91148A module

Overview of adding an X91148A module - AFF A700

You can add an I/O module to your system by either replacing a NIC or storage adapter with a new one in a fully-populated system, or by adding a new NIC or storage adapter into an empty chassis slot in your system.

Before you begin

- Check the [NetApp Hardware Universe](#) to make sure that the new I/O module is compatible with your system and version of ONTAP you're running.
- If multiple slots are available, check the slot priorities in [NetApp Hardware Universe](#) and use the best one available for your I/O module.
- To non-disruptively add an I/O module, you must takeover the target controller, remove the slot blanking cover in the target slot or remove an existing I/O module, add the new or replacement I/O module, and then giveback the target controller.
- Make sure that all other components are functioning properly.

Add an X91148A module in a system with open slots - A700

You can add an X91148A module into an empty module slot in your system as either a 100GbE NIC or a storage module for the NS224 storage shelves.

- Your system must be running ONTAP 9.8 and later.
- To non-disruptively add the X91148A module, you must takeover the target controller, remove the slot blanking cover in the target slot, add the module, and then giveback the target controller.
- There must be one or more open slots available on your system.
- If multiple slots are available, install the module according to the slot priority matrix for the X91148A module in the [NetApp Hardware Universe](#).
- If you are adding the X91148A module as a storage module, you must install the module slots 3 and/or 7.
- If you are adding the X91148A module as a 100GbE NIC, you can use any open slot. However, by default, slots 3 and 7 are set as storage slots. If you wish to use those slots as network slots and will not add NS224 shelves, you must modify the slots for networking use with the `storage port modify -node node name -port port name -mode network` command. See the [NetApp Hardware Universe](#) for other slots that can be used by the X91148A module for networking.
- All other components in the system must be functioning properly; if not, you must contact technical support.

Option 1: Add an X91148A module as a NIC module

To add an X91148A module as a NIC module in a system with open slots, you must follow the specific sequence of steps.

Steps

1. Shutdown controller A:

- a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`
- b. Take over the target node: `storage failover takeover -ofnode target_node_name`

The console connection shows that the node drops to the LOADER prompt when the takeover is complete.

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

3. Remove the target slot blanking cover:

- a. Depress the lettered and numbered cam button.
- b. Rotate the cam latch down until it is in a horizontal position.
- c. Remove the blanking cover.

4. Install the X91148A module:

- a. Align the X91148A module with the edges of the slot.
- b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
- c. Push the I/O cam latch all the way up to lock the module in place.

5. Cable the module to the data switches.

6. Reboot controller A from the LOADER prompt: `bye`



This reinitializes the PCIe cards and other components and reboots the node.

7. Giveback the node from the partner node: `storage failover giveback -ofnode target_node_name`

8. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto-giveback true`

9. Repeat these steps for controller B.

Option 2: Add an X91148A module as a storage module

To add an X91148A module as a storage module in a system with open slots, you must follow the specific sequence of steps.

- This procedure presumes slots 3 and/or 7 are open.

Steps

1. Shut down controller A:

- a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`

b. Take over the target node: `storage failover takeover -ofnode target_node_name`

The console connection shows that the node drops to the LOADER prompt when the takeover is complete.

2. If you are not already grounded, properly ground yourself.
3. Remove the target slot blanking cover:
 - a. Depress the lettered and numbered cam button.
 - b. Rotate the cam latch down until it is in a horizontal position.
 - c. Remove the blanking cover.
4. Install the X91148A module into slot 3:
 - a. Align the X91148A module with the edges of the slot.
 - b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
 - c. Push the I/O cam latch all the way up to lock the module in place.
 - d. If you are installing a second X91148A module for storage, repeat this step for the module in slot 7.
5. Reboot controller A:
 - If the replacement module is not the same model as the old module, reboot the BMC :
 - a. From the LOADER prompt, change to advanced privilege mode: `set -privilege advanced`
 - b. Reboot the BMC: `sp reboot`
 - If the replacement module is the same as the old module, boot from the LOADER prompt: `bye`



This reinitializes the PCIe cards and other components and reboots the node.

6. Giveback the node from the partner node: `storage failover giveback -ofnode target_node_name`
7. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto-giveback true`
8. Repeat these steps for controller B.
9. Install and cable your NS224 shelves, as described in [Hot-add workflow](#).

Add an X91148A storage module in a system with no open slots - A700

You must remove one more or more existing NIC or storage modules in your system in order to install one or more X91148A storage modules into your fully-populated system.

- Your system must be running ONTAP 9.8 and later.
- To non-disruptively add the X91148A module, you must takeover the target controller, add the module, and then giveback the target controller.
- If you are adding the X91148A module as a storage adapter, you must install the module in slots 3 and/or 7.

- If you are adding the X91148A module as a 100GbE NIC, you can use any open slot. However, by default, slots 3 and 7 are set as storage slots. If you wish to use those slots as network slots and will not add NS224 shelves, you must modify the slots for networking use with the `storage port modify -node node name -port port name -mode network` command for each port. See the [NetApp Hardware Universe](#) for other slots that can be used by the X91148A module for networking.
- All other components in the system must be functioning properly; if not, you must contact technical support.

Option 1: Add an X91148A module as a NIC module

You must remove one or more existing NIC or storage modules in your system in order to install one or more X91148A NIC modules into your fully-populated system.

Steps

1. If you are adding an X91148A module into a slot that contains a NIC module with the same number of ports as the X91148A module, the LIFs will automatically migrate when its controller module is shut down. If the NIC module being replaced has more ports than the X91148A module, you must permanently reassign the affected LIFs to a different home port. See [Migrating a LIF](#) for information about using System Manager to permanently move the LIFs

2. Shut down controller A:

- a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`

- b. Take over the target node: `storage failover takeover -ofnode target_node_name`

The console connection shows that the node drops to the LOADER prompt when the takeover is complete.

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

4. Unplug any cabling on the target I/O module.

5. Remove the target I/O module from the chassis:

- a. Depress the lettered and numbered cam button.

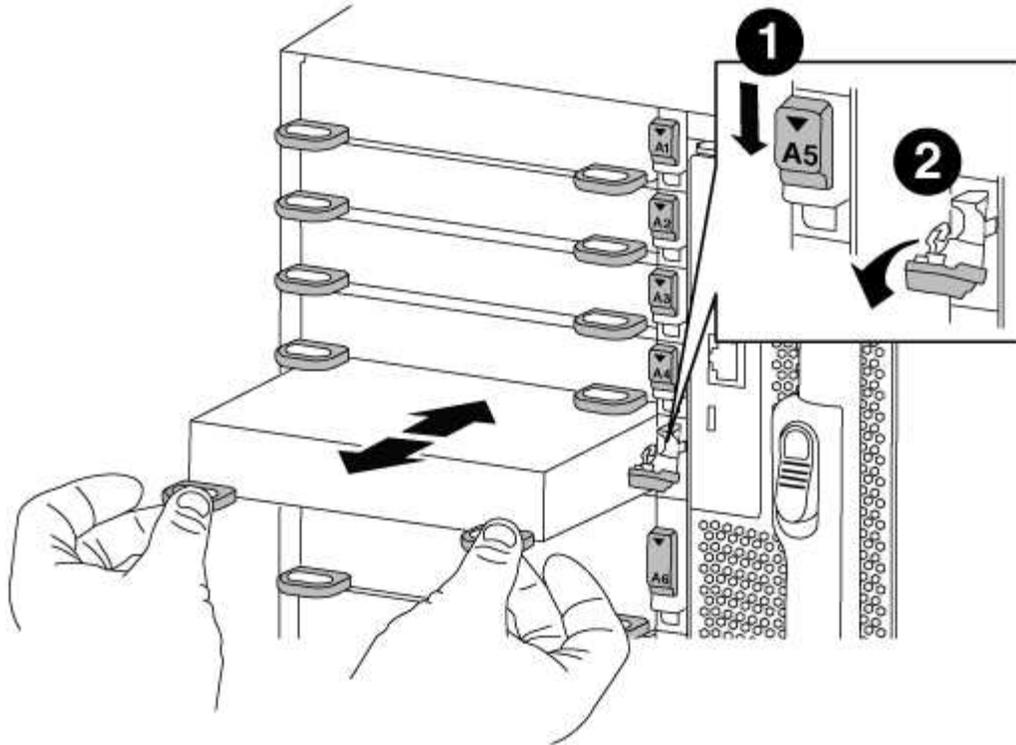
The cam button moves away from the chassis.

- b. Rotate the cam latch down until it is in a horizontal position.

The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

- c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

Make sure that you keep track of which slot the I/O module was in.



<p>1</p>	<p>Lettered and numbered I/O cam latch</p>
<p>2</p>	<p>I/O cam latch completely unlocked</p>

6. Install the X91148A module into the target slot:
 - a. Align the X91148A module with the edges of the slot.
 - b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
 - c. Push the I/O cam latch all the way up to lock the module in place.
7. Repeat the remove and install steps to replace additional modules for controller A.
8. Cable the module or modules to the data switches.
9. Reboot controller A from the LOADER prompt: `bye`



This reinitializes the PCIe cards and other components and reboots the node.

10. Giveback the node from the partner node: `storage failover giveback -ofnode target_node_name`
11. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto-giveback true`
12. If you added the X91148A module as a NIC module in slots 3 or 7, for networking, use the `storage port modify -node node name -port port name -mode network` command for each port.

13. Repeat these steps for controller B.

Option 2: Adding an X91148A module as a storage module

You must remove one or more existing NIC or storage modules in your system in order to install one or more X91148A storage modules into your fully-populated system.

- This procedure presumes you re installing the X91148A module into slots 3 and/or 7.

Steps

1. If you are adding an X91148A module as a storage module in slots 3 and/or 7 into a slot that has an existing NIC module in it, use System Manager to permanently migrate the LIFs to different home ports, as described in [Migrating a LIF](#).

2. Shut down controller A:

a. Disable automatic giveback: `storage failover modify -node local -auto-giveback false`

b. Take over the target node: `storage failover takeover -ofnode target_node_name`

The console connection shows that the node drops to the LOADER prompt when the takeover is complete.

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

4. Unplug any cabling on the target I/O module.

5. Remove the target I/O module from the chassis:

a. Depress the lettered and numbered cam button.

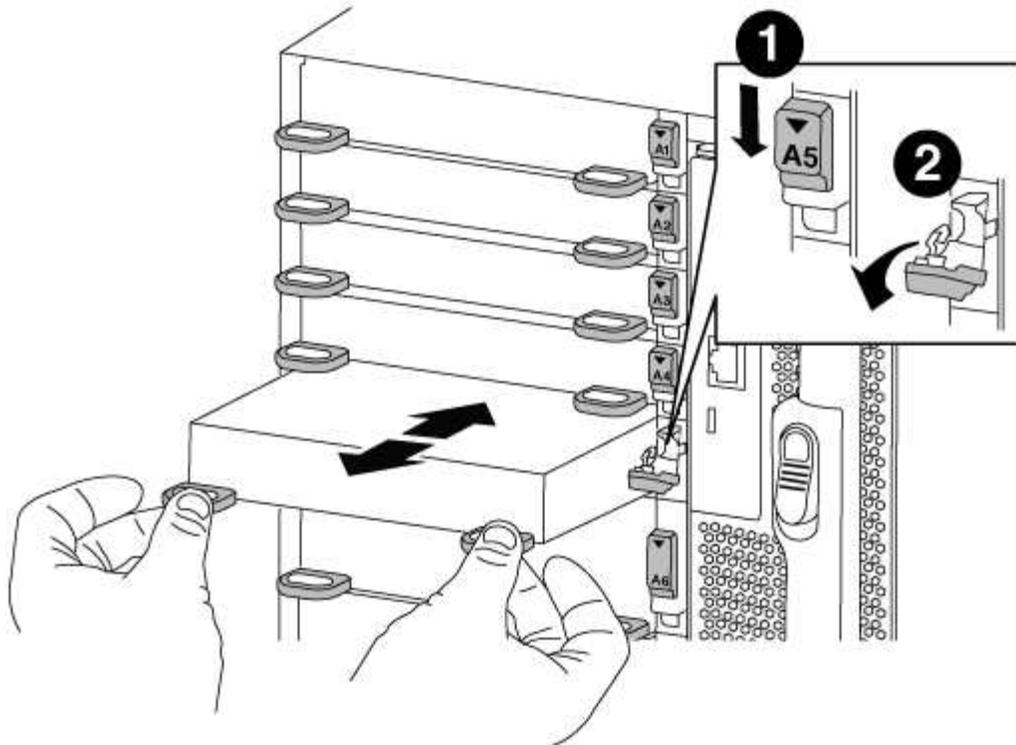
The cam button moves away from the chassis.

b. Rotate the cam latch down until it is in a horizontal position.

The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

c. Remove the I/O module from the chassis by pulling on the pull tabs on the sides of the module face.

Make sure that you keep track of which slot the I/O module was in.



<p>1</p>	<p>Lettered and numbered I/O cam latch</p>
<p>2</p>	<p>I/O cam latch completely unlocked</p>

6. Install the X91148A module into slot 3:

- a. Align the X91148A module with the edges of the slot.
- b. Slide the X91148A module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
- c. Push the I/O cam latch all the way up to lock the module in place.
- d. If you are installing a second X91148A module for storage, repeat the remove and install steps for the module in slot 7.

7. Reboot controller A from the LOADER prompt: `bye`



This reinitializes the PCIe cards and other components and reboots the node.

8. Giveback the node from the partner node: `storage failover giveback -ofnode target_node_name`

9. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto-giveback true`

10. Repeat these steps for controller B.

11. Install and cable your NS224 shelves, as described in [Hot-add workflow](#).

Copyright information

Copyright © 2026 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, 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) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.