# FAS systems

## ONTAP Systems

NetApp
June 13, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap-systems/fas500f/install-setup.html on June 13, 2022. Always check docs.netapp.com for the latest.

# Table of Contents

FAS systems . . . 1
- FAS500f System Documentation . . . 1
- FAS2600 System Documentation . . . 90
- FAS2700 System Documentation . . . 174
- FAS8200 System Documentation . . . 289
- FAS8300 and FAS8700 System Documentation . . . 408
- FAS9000 System Documentation . . . 537
- FAS9500 systems . . . 683

# FAS systems

## FAS500f System Documentation

### Install and setup

#### Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

If your system is in a MetroCluster IP configuration, see the Install MetroCluster IP Configuration instructions.

#### Quick steps - FAS500f

This section gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

- English: FAS500f Installation and Setup Instructions
- Japanese: FAS500f Systems Installation and Setup Instructions
- Chinese: FAS500f Systems Installation and Setup Instructions

#### Videos - FAS500f

There are two videos - one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

##### Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

Installation and Setup of a FAS500f

#### Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

### Detailed steps - FAS500f

## This section gives detailed step-by-step instructions for installing a FAS500f system.

#### Step 1: Prepare for installation

To install your FAS500f system, you need to create an account and register the system. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

You need to have access to the NetApp Hardware Universe (HWU) for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

**What you need**

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser

**Steps**

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Set up your account:
   a. Log in to your existing account or create an account.
   b. Register (NetApp Product Registration) your system.
4. Download and install NetApp Downloads: Config Advisor on your laptop.
5. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the NetApp Hardware Universe to locate the cable and identify its use.

| Type of cable… | Part number and length | Connector type | For… |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 25 GbE cable | X66240A-05 (112-00595), 0.5m;<br><br>X66240-2 (112-00573), 2m | | Cluster interconnect network |
| | X66240A-2 (112-00598), 2m;<br><br>X66240A-5 (112-00600), 5m | | Data |
| 100 GbE cable | X66211-2 (112-00574), 2m;<br><br>X66211-5 (112-00576), 5m | | Storage |
| RJ-45 (order dependent) | Not applicable | | Management network (BMC and wrench port) and Ethernet data (e0a and e0b) |
| Fibre Channel | X66250-2 (112-00342) 2m;<br><br>X66250-5 (112-00344) 5m;<br><br>X66250-15 (112-00346) 15m;<br><br>X66250-30 (112-00347) 30m | | |
| Micro-USB console cable | Not applicable | | Console connection during software setup |
| Power cables | Not applicable | | Powering up the system |

1. Review the ONTAP Configuration Guide and collect the required information listed in that guide.

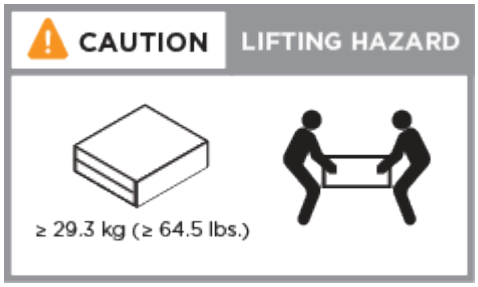
#### Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

**Steps**

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

You need to be aware of the safety concerns associated with the weight of the system.




3. Identify and manage cables because this system does not have a cable management device.
4. Place the bezel on the front of the system.

#### Step 3: Cable controllers

There is required cabling for your platform's cluster using the two-node switchless cluster method or the cluster interconnect network method. There is optional cabling to the Fibre Channel or iSCSI host networks or direct-attached storage. This cabling is not exclusive; you can have cable to a host network and storage.

### Required cabling: Cable controllers to a cluster

Cable the controllers to a cluster by using the two-node switchless cluster method or by using the cluster interconnect network.

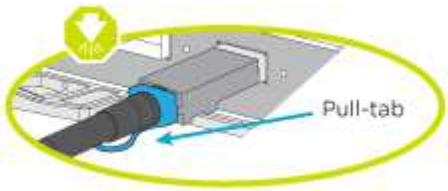
### Option 1: Cable a two-node switchless cluster

The management, Fibre Channel, and data or host network ports on the controller modules are connected to switches. The cluster interconnect ports are cabled on both controller modules.

#### Before you begin

Contact your network administrator for information about connecting the system to the switches.

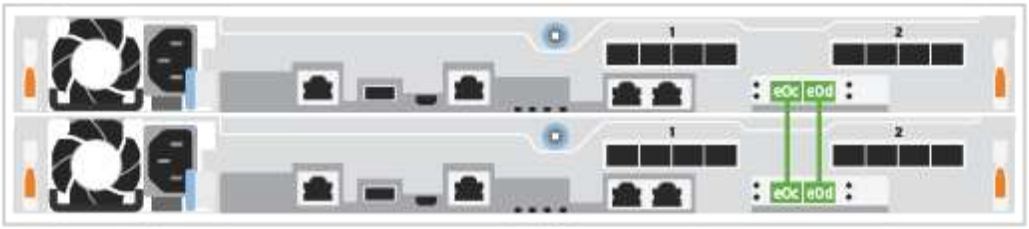
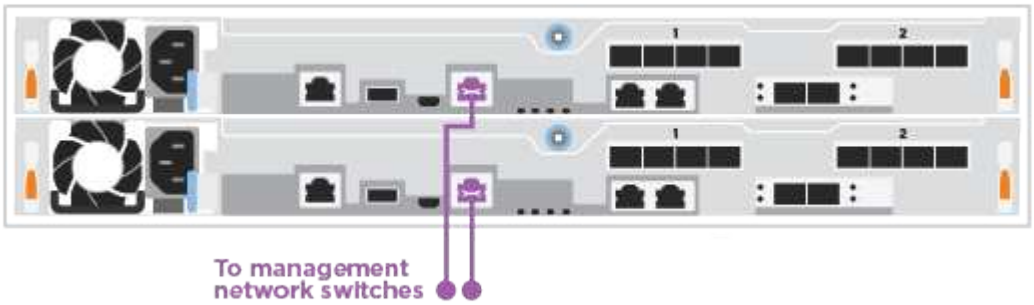
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.




As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

#### Steps

1. Use the animation (Cable a two-node switchless cluster) or the step-by-step instructions to complete the cabling between the controllers and to the switches:

| Step | Perform on each controller |
|---|---|
| 1 | Cable the cluster interconnect ports to each other with the 25GbE cluster interconnect cable :<br>• e0c to e0c<br>• e0d to e0d<br>  |
| 2 | Cable the wrench ports to the management network switches with the RJ45 cables.<br>  |
| ! | DO NOT plug in the power cords at this point. |

2. To complete setting up your system, see Step 4: Complete system setup and configuration.

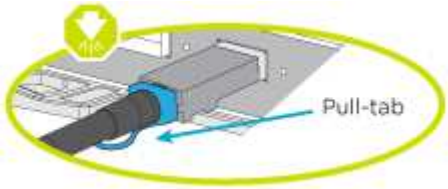
### Option 2: Cable a switched cluster

All ports on the controllers are connected to switches; cluster interconnect, management, Fibre Channel, and data or host network switches.

#### Before you begin

Contact your network administrator for information about connecting the system to the switches.

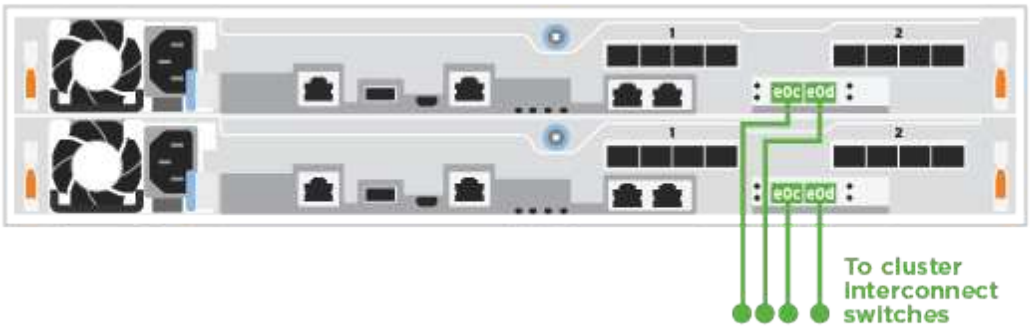
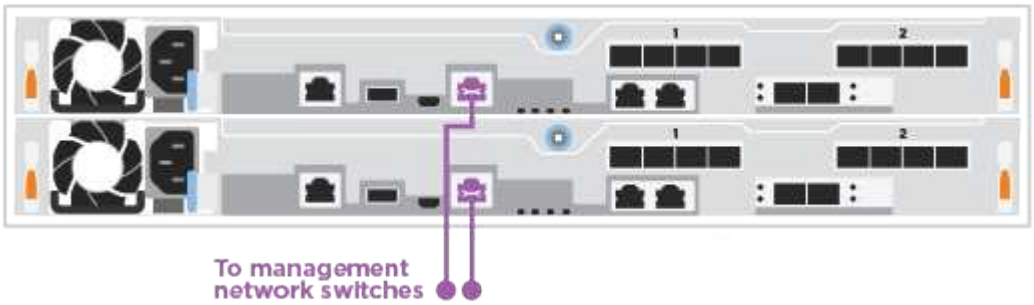
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.



As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. Use the animation (Cabling a switched cluster) or the step-by-step instructions to complete the cabling between the controllers and to the switches:

| Step | Perform on each controller |
|---|---|
| 1 | Cable the cluster interconnect ports to the 25 GbE cluster interconnect switches.<br>• e0c<br>• e0d<br>  |
| 2 | Cable the wrench ports to the management network switches with the RJ45 cables.<br>  |
| ! | DO NOT plug in the power cords at this point. |

2. To complete setting up your system, see Step 4: Complete system setup and configuration.

### Optional cabling: Cable configuration-dependent options

You have configuration-dependent optional cabling to the Fibre Channel or iSCSI host networks or direct-attached storage. This cabling is not exclusive; you can have cabling to a host network and storage.

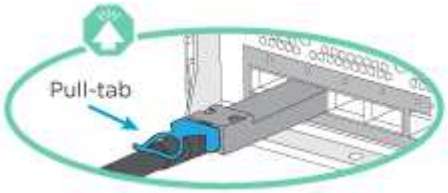
### Option 1: Cable to a Fibre Channel host network

Fibre Channel ports on the controllers are connected to Fibre Channel host network switches.

**Before you begin**

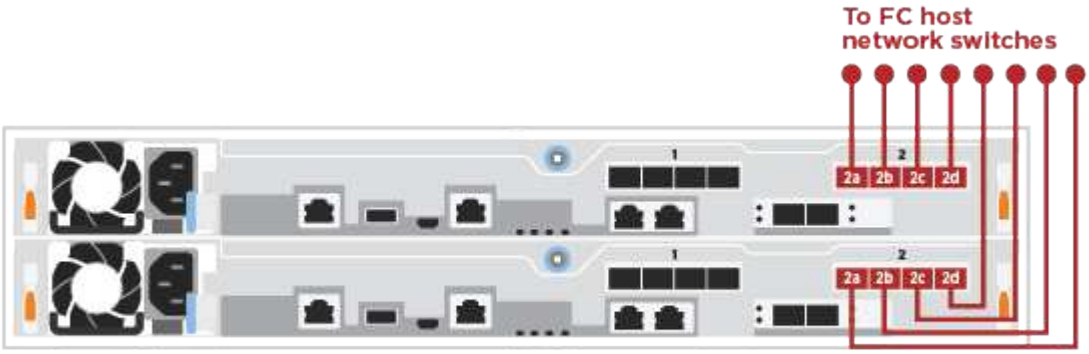
Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.




As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

+

| Step | Perform on each controller module |
|---|---|
| 1 | Cable ports 2a through 2d to the FC host switches.<br>  <br> |
| 2 | To perform other optional cabling, choose from:<br>• Option 2: Cable to a 25GbE data or host network<br>• Option 3: Cable the controllers to a single drive shelf |
| 3 | To complete setting up your system, see Step 4: Complete system setup and configuration. |

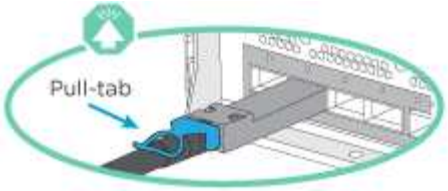
**Option 2: Cable to a 25GbE data or host network**

25GbE ports on the controllers are connected to 25GbE data or host network switches.

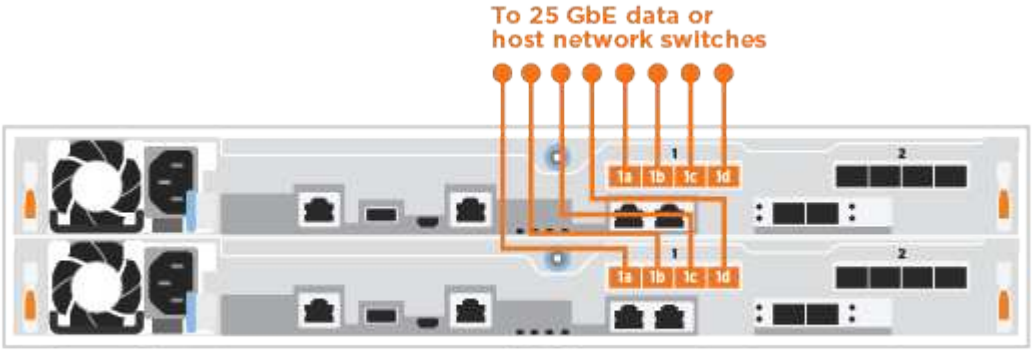
**Before you begin**

Contact your network administrator for information about connecting the system to the switches.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.



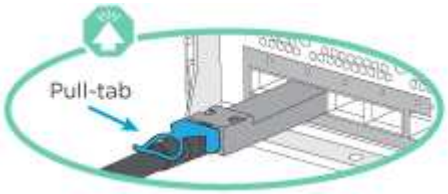

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

| Step | Perform on each controller module |
|---|---|
| 1 | Cable ports e4a through e4d to the 10GbE host network switches.<br>  <br> |
| 2 | To perform other optional cabling, choose from:<br>• Option 1: Cable to a Fibre Channel host network<br>• Option 3: Cable the controllers to a single drive shelf |
| 3 | To complete setting up your system, see Step 4: Complete system setup and configuration. |

### Option 3: Cable the controllers to a single drive shelf

You must cable each controller to the NSM modules on the NS224 drive shelf.

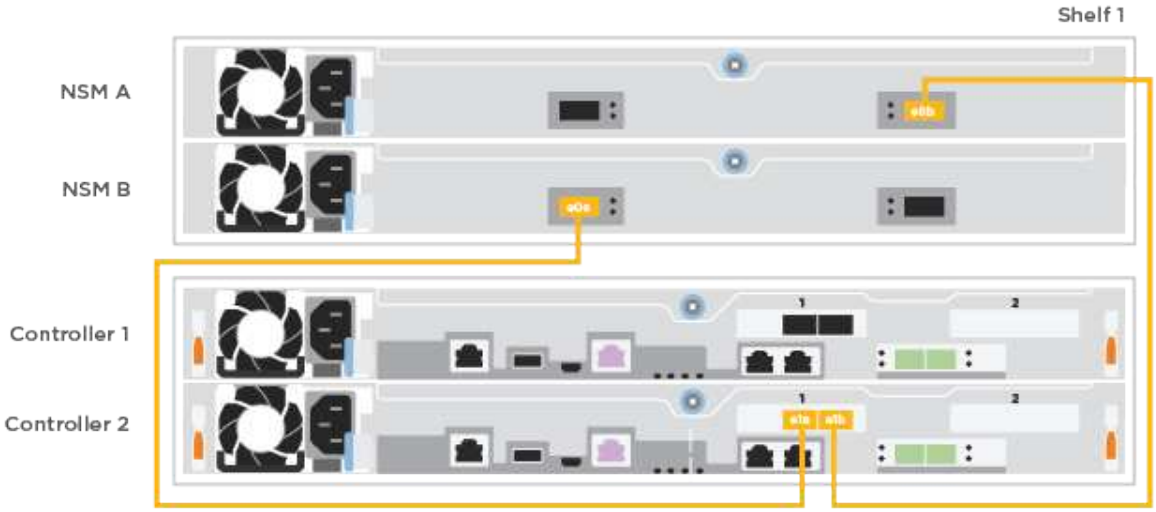
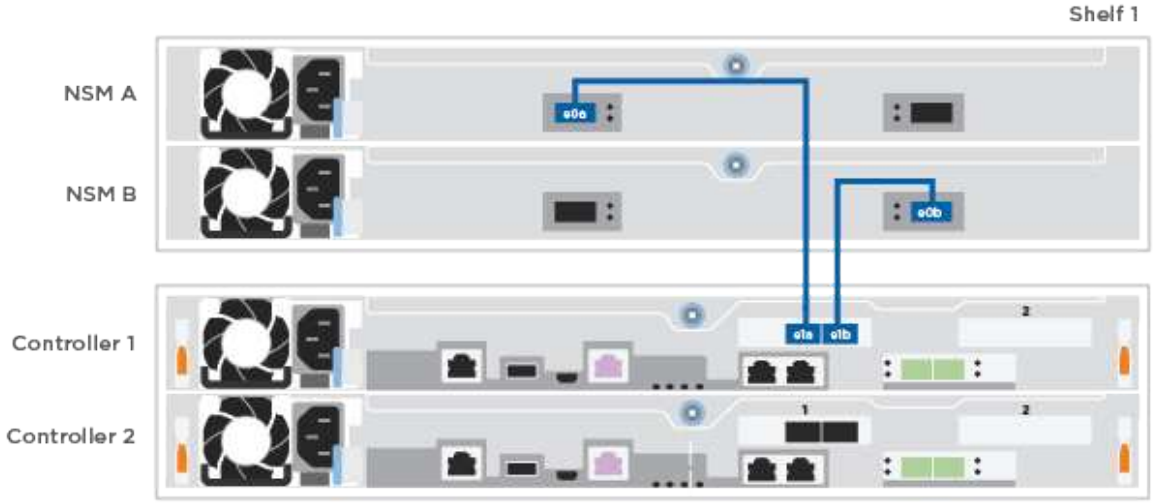
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.




As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. Use the animation (Cabling the controllers to a single NS224) or the step-by-step instructions to cable your controller modules to a single shelf.

| Step | Perform on each controller module |
|---|---|
| 1 | Cable controller A to the shelf:   |
| 2 | Cable controller B to the shelf:   |

2. To complete setting up your system, see Step 4: Complete system setup and configuration.

#### Step 4: Complete system setup and configuration

Complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

### Option 1: Complete system setup and configuration if network discovery is enabled

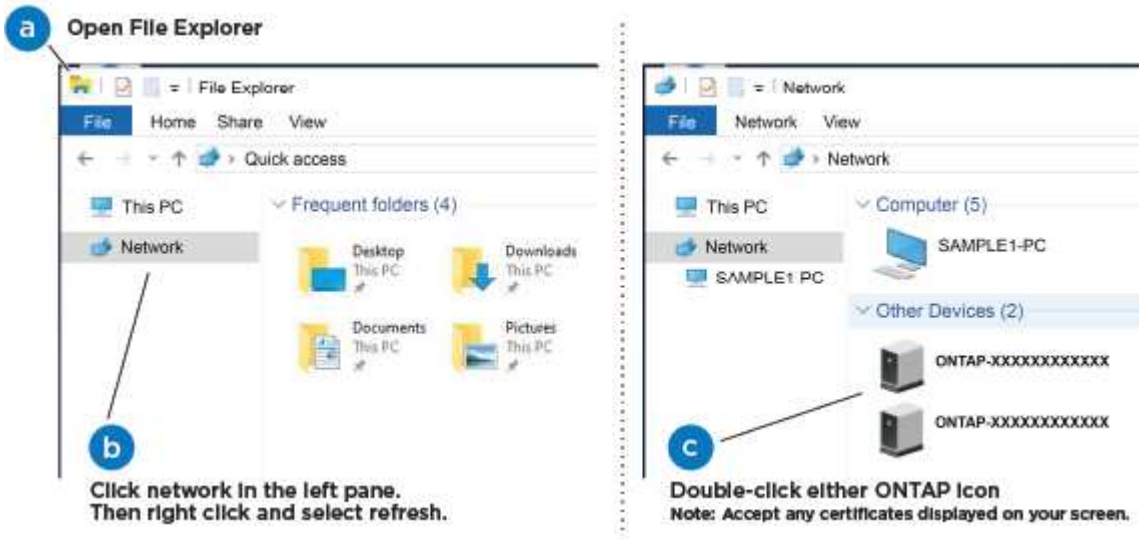
If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

**Steps**

1. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
2. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

3. Use the animation (Connecting your laptop to the Management switch) to connect your laptop to the Management switch.
4. Select an ONTAP icon listed to discover:




   a. Open File Explorer.
   b. Click **Network** in the left pane.
   c. Right-click and select **refresh**.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

   > XXXXX is the system serial number for the target node.

   System Manager opens.

5. Use System Manager guided setup to configure your system using the data you collected in the ONTAP Configuration Guide.
6. Verify the health of your system by running Config Advisor.
7. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

### Option 2: Complete system setup and configuration if network discovery is not enabled

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

**Steps**

1. Cable and configure your laptop or console:

a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

> See your laptop or console's online help for how to configure the console port.

b. Connect the laptop or console to the switch on the management subnet.

c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Assign an initial node management IP address to one of the nodes.

| If the management network has DHCP… | Then… |
|---|---|
| Configured | Record the IP address assigned to the new controllers. |
| Not configured | a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment.<br>Check your laptop or console's online help if you do not know how to configure PuTTY.<br>b. Enter the management IP address when prompted by the script. |

4. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

   > The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the ONTAP Configuration Guide.
5. Verify the health of your system by running Config Advisor.
6. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

## Maintain

### Boot media

#### Overview of boot media replacement - FAS500f

## The boot media stores a primary and secondary set of system (boot image) files that the system uses when it boots.

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

- 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 controller:
  - The *impaired* controller is the controller on which you are performing maintenance.
  - The *healthy* controller is the HA partner of the impaired controller.

#### Check onboard encryption keys - FAS500f

## Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check what version of ONTAP the system is running.

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

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 the NetApp Encryption overview with the CLI.

**Steps**

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. 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`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to the next section.

4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

### Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

### Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`

e. Shut down the impaired controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

   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.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

   c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

### Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.

- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
   a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   b. Enter the command to display the key management information: `security key-manager onboard show-backup`
   c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   d. Return to admin mode: `set -priv admin`
   e. You can safely shut down the controller.
2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

#### Shut down the controller - FAS500f

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller. Shut down or take over the impaired controller using the appropriate procedure for your configuration.

**Option 1: Most configurations**

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 `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name`<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

1. 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**

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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### Replace the boot media - FAS500f

## 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.

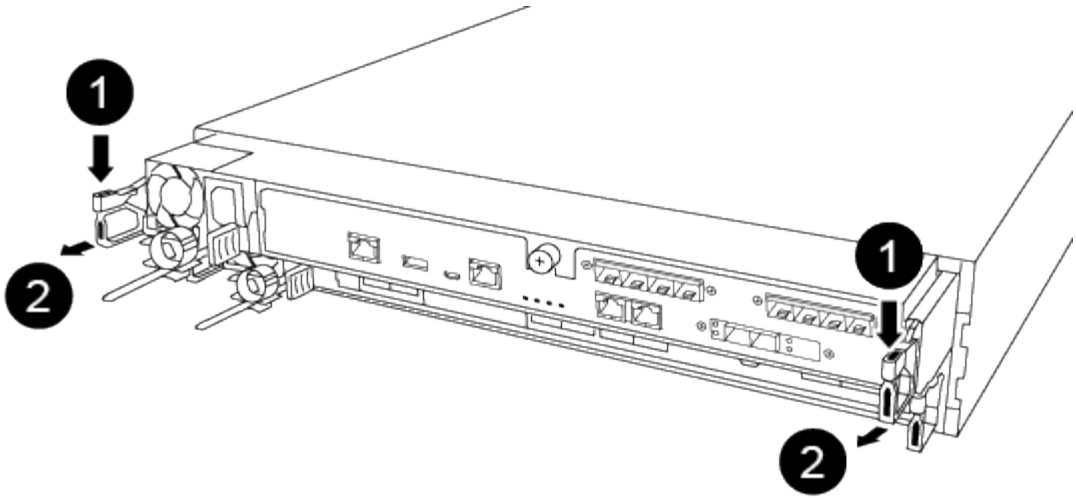
### Step 1: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

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

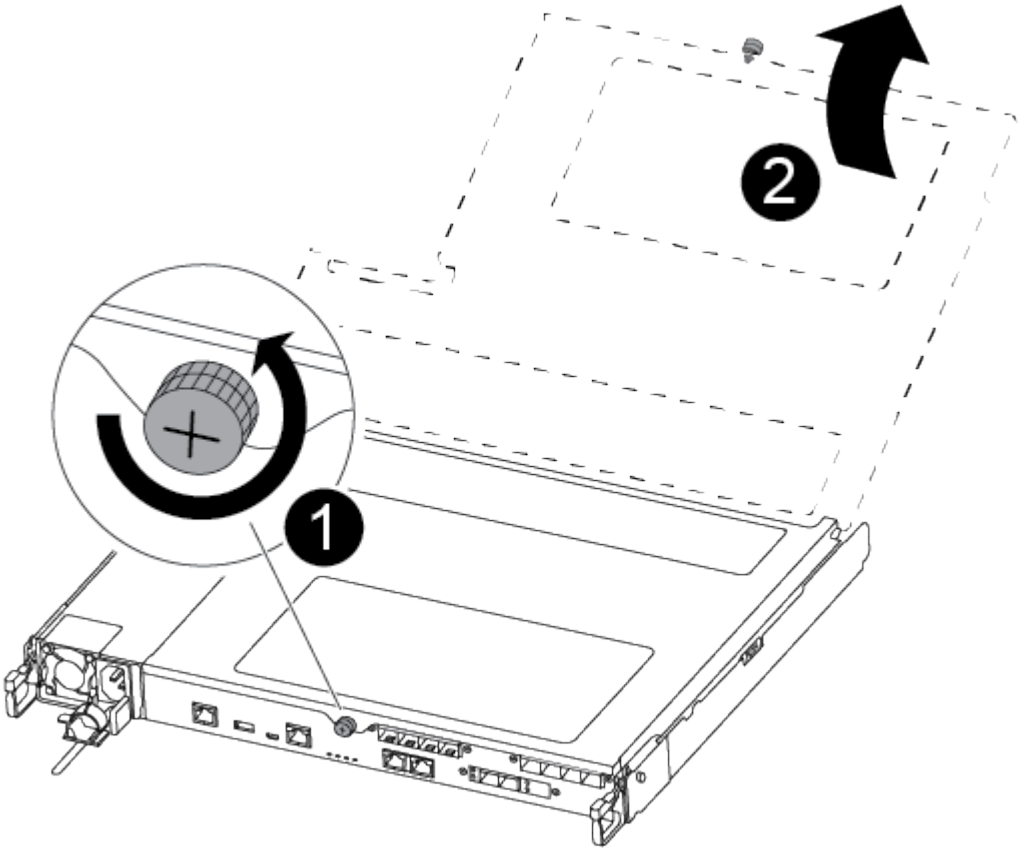
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

   > If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



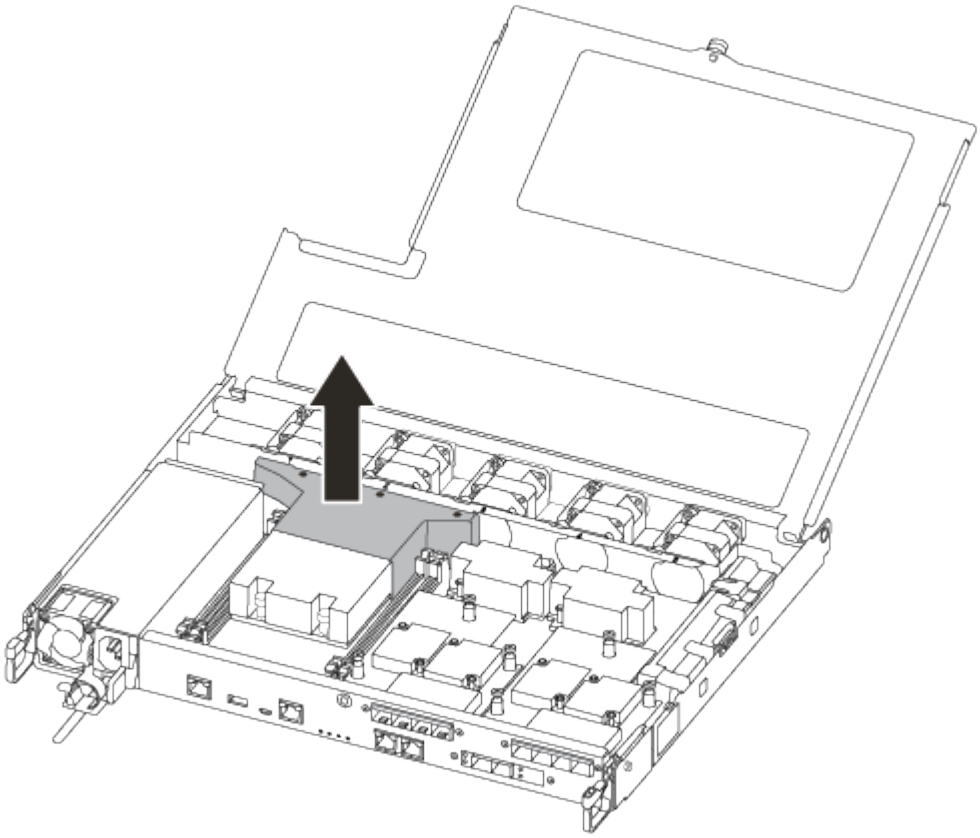
| | |
|---|---|
| 1 | Lever |
| 2 | Latching mechanism |

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.



| | |
|---|---|
| ❶ | Thumbscrew |
| ❷ | Controller module cover. |

7. Lift out the air duct cover.



**Step 2: Replace the boot media**

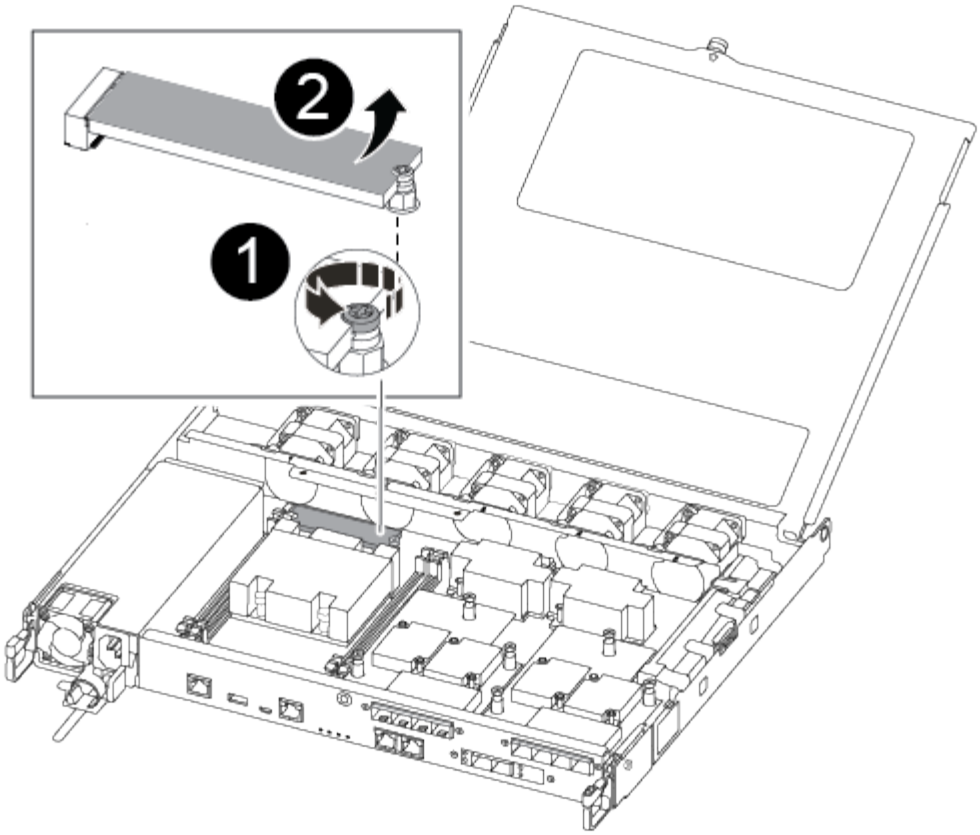
You locate the failed boot media in the controller module by removing the air duct on the controller module before you can replace the boot media.

You need a #1 magnetic Phillips head screwdriver to remove the screw that holds the boot media in place. Due to the space constraints within the controller module, you should also have a magnet to transfer the screw on to so that you do not loose it.

You can use the following video or the tabulated steps to replace the boot media:

Replacing the boot media

1. Locate and replace the impaired boot media from the controller module.



| | |
|---|---|
| 1 | Remove the screw securing the boot media to the motherboard in the controller module. |
| 2 | Lift the boot media out of the controller module. |

a. Using the #1 magnetic screwdriver, remove the screw from the impaired boot media, and set it aside safely on the magnet.

b. Gently lift the impaired boot media directly out of the socket and set it aside.

c. Remove the replacement boot media from the antistatic shipping bag and align it into place on the controller module.

d. Using the #1 magnetic screwdriver, insert and tighten the screw on the boot media.

> Do not apply force when tightening the screw on the boot media; you might crack it.

**Step 3: Transfer the boot image to the boot media**

The replacement boot media that you installed is without a boot image so you need to transfer a boot image using a USB flash drive.

- You must have a USB flash drive, formatted to MBR/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 an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

**Steps**

1. Download and copy the appropriate service image from the NetApp Support Site to the USB flash drive.
2. Download the service image to your work space on your laptop.
3. Unzip the service image.

   > If you are extracting the contents using Windows, do not use WinZip to extract the netboot image. Use another extraction tool, such as 7-Zip or WinRAR.

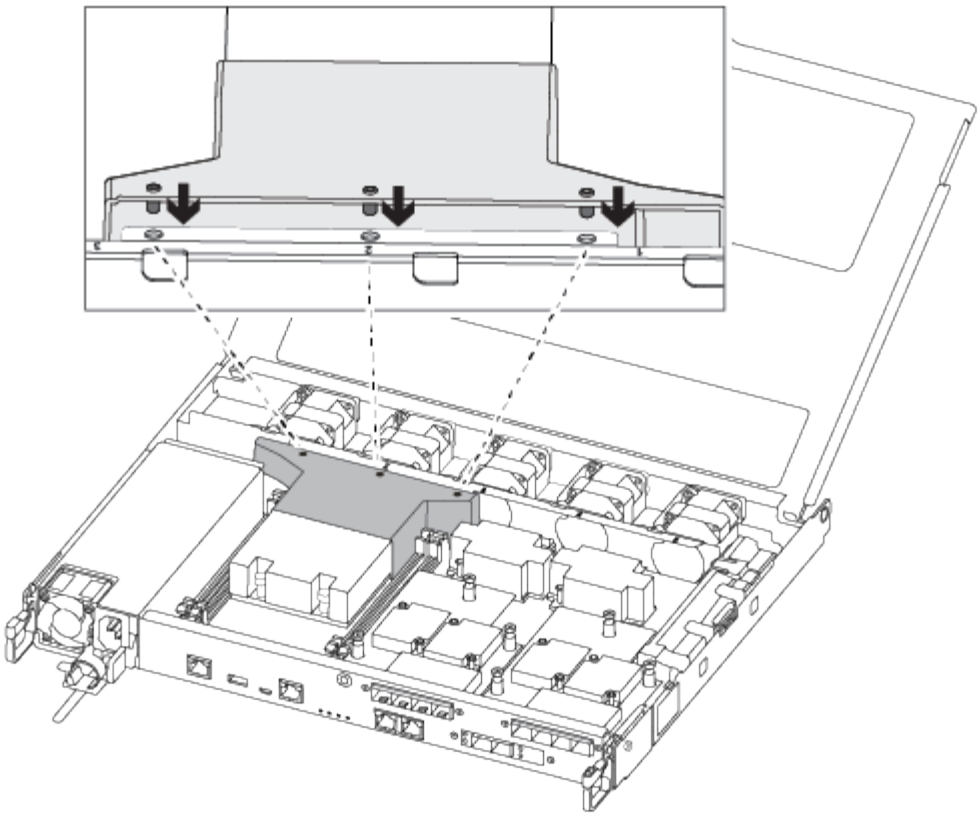
   There are two folders in the unzipped service image file:

   - `boot`
   - `efi`

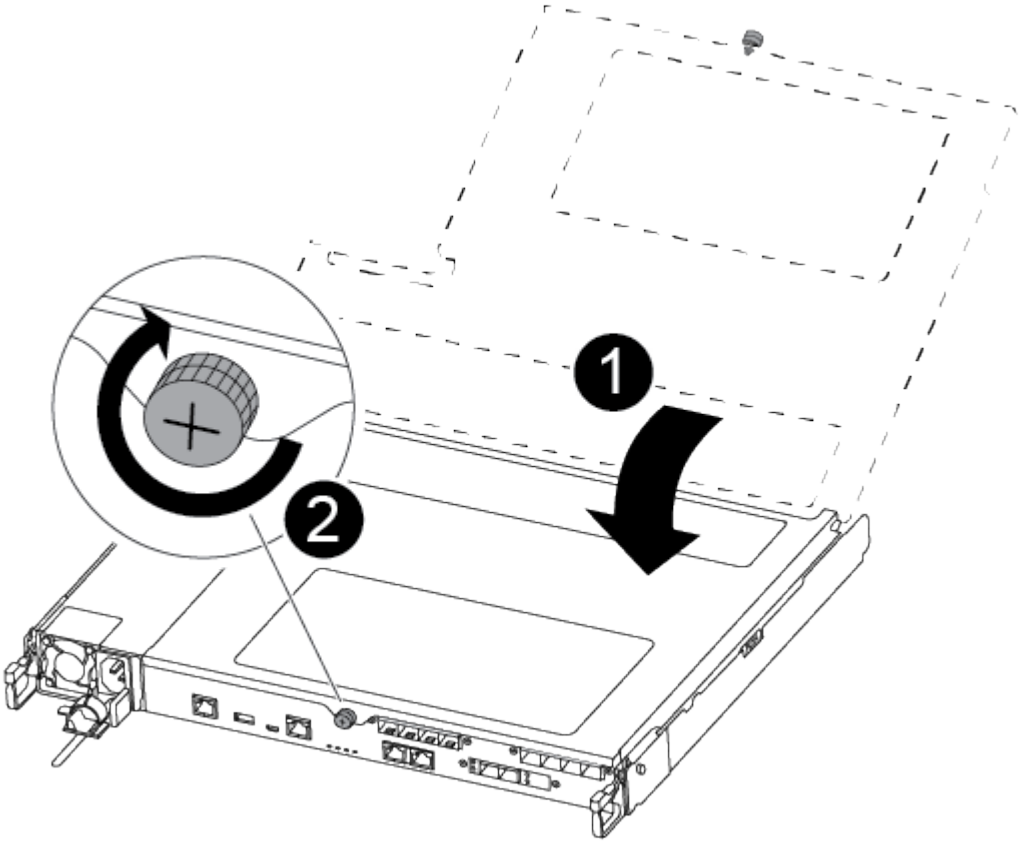
4. Copy the `efi` folder to the top directory on the USB flash drive.

   The USB flash drive should have the efi folder and the same Service Image (BIOS) version of what the impaired controller is running.

5. Remove the USB flash drive from your laptop.
6. If you have not already done so, install the air duct.



7. Close the controller module cover and tighten the thumbscrew.



| | |
|---|---|
| ❶ | Controller module cover |
| ❷ | Thumbscrew |

8. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
9. Plug the power cable into the power supply and reinstall the power cable retainer.
10. 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.

11. Push the controller module all the way into the chassis:
12. Place your index fingers through the finger holes from the inside of the latching mechanism.
13. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
14. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

    The controller module should be fully inserted and flush with the edges of the chassis.

#### Boot the recovery image - FAS500f

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

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

| If your system has… | Then… |
| --- | --- |
| No network connection and is in a MetroCluster IP configuration | a. Press `n` when prompted to restore the backup configuration.<br>b. Reboot the system when prompted by the system.<br>c. Wait for the iSCSI storage connections to connect.<br>You can proceed after you see the following messages:<br>`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).`<br>`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).`<br>`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).`<br>`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).`<br>d. Select the **Update flash from backup config** (sync flash) option from the displayed menu.<br>If you are prompted to continue with the update, press `y`. |

4. Ensure that the environmental variables are set as expected:
   a. Take the controller 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 controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

7. Connect the console cable to the partner controller.
8. Give back the controller 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 controller 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.

#### Restore OKM, NSE, and NVE as needed - FAS500f

## Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

1. Determine which section you should use to restore your OKM, NSE, or NVE configurations: If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.
   - If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Restore NVE or NSE when Onboard Key Manager is enabled.
   - If NSE or NVE are enabled for ONTAP 9.6, go to Restore NSE/NVE on systems running ONTAP 9.6 and later.

### Restore NVE or NSE when Onboard Key Manager is enabled

#### Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
| --- | --- |
| The LOADER prompt | Boot the controller to the boot menu: `boot_ontap menu` |
| Waiting for giveback…. | a. Enter `Ctrl-C` at the prompt<br>b. At the message: Do you wish to halt this node rather than wait [y/n]? , enter: `y`<br>c. At the LOADER prompt, enter the `boot_ontap menu` command. |

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command

> The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

Example of backup data:

```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rlbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```

7. At the Boot Menu select the option for Normal Boot.

   The system boots to Waiting for giveback… prompt.

8. Move the console cable to the partner controller and login as "admin".

9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Giveback only the CFO aggregates with the `storage failover giveback -fromnode local -only-cfo-aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

      Terminating CIFS can cause loss of data.

    - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `storage failover show`-giveback` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
    a. If you are running ONTAP 9.6 or later, run the security key-manager onboard sync:
    b. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    c. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    d. Wait 10 minutes for the key to synchronize across the cluster.
13. Move the console cable to the partner controller.
14. Give back the target controller using the `storage failover giveback -fromnode local` command.
15. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

16. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

17. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
18. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

### Restore NSE/NVE on systems running ONTAP 9.6 and later

#### Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
|---|---|
| The login prompt | Go to Step 7. |
| Waiting for giveback… | a. Log into the partner controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

   If any interfaces are listed as `false`, revert those interfaces back to their home port using the `net int revert` command.
7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.

- If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

  > If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

  Use the `security key-manager key query` command to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

#### Return the failed part to NetApp - FAS500f

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Chassis

#### Overview of chassis replacement - FAS500f

To replace the chassis, you must move the bezel, controller modules, and NVMe drives from the impaired chassis to the replacement chassis, and then remove the impaired chassis from the equipment rack or system cabinet and install the replacement chassis in its place.

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 written with the assumption that you are moving the bezel, NVMe drives, and controller modules to the new chassis, and that the replacement chassis is a new component from NetApp.
- 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 - FAS500f

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

**About this task**

- If you have a cluster with more than two controllers, 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 the Administration overview with the CLI.
- 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`

**Steps**

1. If your system has two controller modules, disable the HA pair.

| If your system is running clustered ONTAP with… | Then… |
|---|---|
| Two controllers in the cluster | `cluster ha modify -configured false` `storage failover modify -node node0 -enabled false` |
| More than two controllers in the cluster | `storage failover modify -node node0 -enabled false` |

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

# Move the power supplies, 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 controller modules

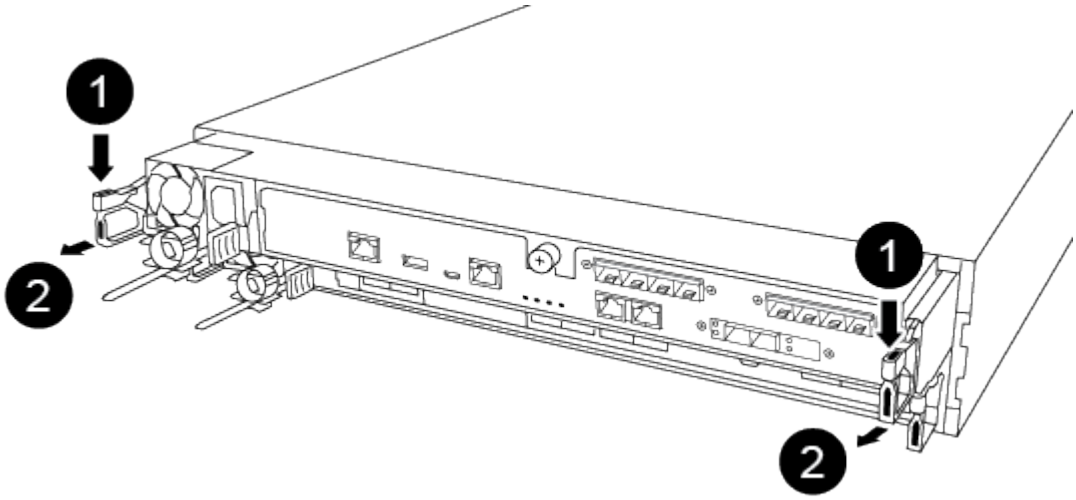
To replace the chassis, you must remove the controller modules from the old chassis.

You can use the following video or the tabulated steps to replace the chassis; it assumes the removal and replacement of the bezel:

Replacing the chassis

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).




| | |
|---|---|
| 1 | Lever |
| 2 | Latching mechanism |

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Set the controller module aside in a safe place, and repeat these steps for the other controller module in the chassis.

### Step 2: Move drives to the new chassis

You need to move the drives from each bay opening in the old chassis to the same bay opening in the new chassis.

1. Gently remove the bezel from the front of the system.
2. Remove the drives:
   a. Press the release button at the top of the carrier face below the LEDs.
   b. Pull the cam handle to its fully open position to unseat the drive from the midplane, and then gently slide the drive out of the chassis.

      The drive should disengage from the chassis, allowing it to slide free of the chassis.

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

      Drives are fragile. Handle them as little as possible to prevent damage to them.
3. Align the drive from the old chassis with the same bay opening in the new chassis.
4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate upward.
5. Firmly push the drive the rest of the way into the chassis, and then lock the cam handle by pushing it up and against the drive holder.

   Be sure to close the cam handle slowly so that it aligns correctly with the front of the drive carrier. It clicks when it is secure.
6. Repeat the process for the remaining drives in the system.

### Step 3: Replace a chassis from within the equipment rack or system cabinet

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.
2. With two people, slide the old chassis off the rack rails in a system cabinet or equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two 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 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. If you have not already done so, install the bezel.

### Step 4: Install the controller modules

After you install the controller modules into the new chassis, you need to boot it to a state where you can run

the diagnostic test.

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.

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. Plug the power cables into the power supplies and reinstall the power cable retainers.
4. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
   c. Place your index fingers through the finger holes from the inside of the latching mechanism.
   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

   The controller module should be fully inserted and flush with the edges of the chassis.

5. Repeat the preceding steps to install the second controller into the new chassis.

#### Complete the restoration and replacement process - FAS500f

## You must verify the HA state of the chassis, run diagnostics, 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.

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`
    - `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. Reinstall the bezel on the front of the system.

### Step 2: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test System** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

### 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 & Replacements page for further information.

## Controller

#### Overview of controller module replacement - FAS500f

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 is in a MetroCluster configuration, you must review the section Choosing the correct recovery procedure to determine whether you should use this procedure.
- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot

upgrade your system by just replacing the controller module.

- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller 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* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller'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 - FAS500f

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### Replace the controller module hardware - FAS500f

To replace the controller module hardware, you must remove the impaired controller, 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

You must remove the controller module from the chassis when you replace a component inside the controller module.

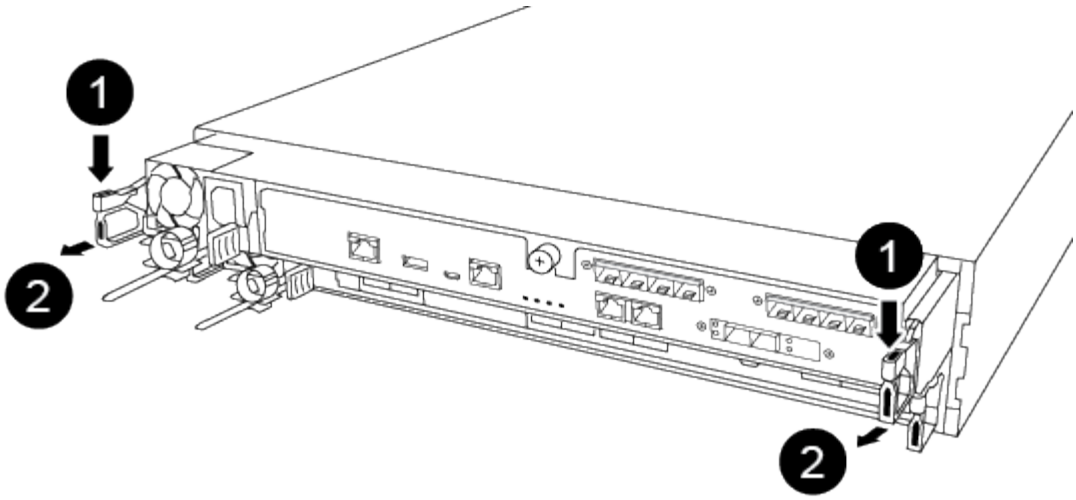
Make sure that you label the cables so that you know where they came from.

You can use the following video or the tabulated steps to replace a controller module:

Replacing a controller module

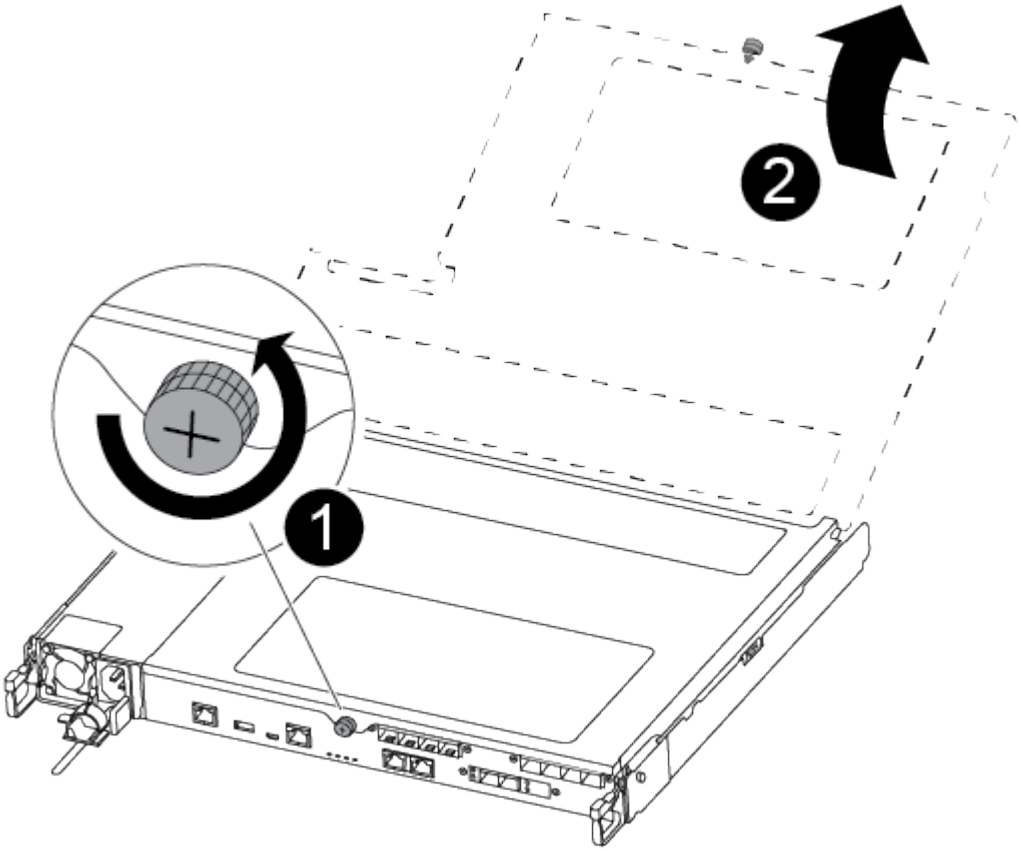
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



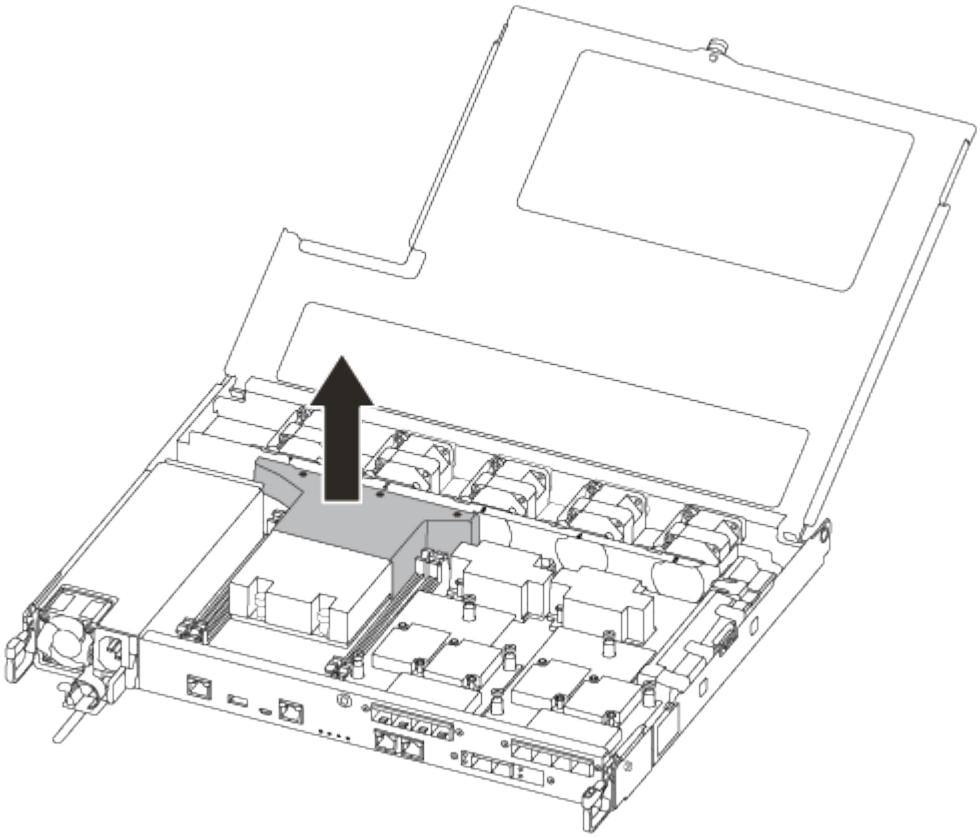
| | |
|---|---|
| 1 | Lever |
| 2 | Latching mechanism |

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.



| | |
|---|---|
| ❶ | Thumbscrew |
| ❷ | Controller module cover. |

7. Lift out the air duct cover.

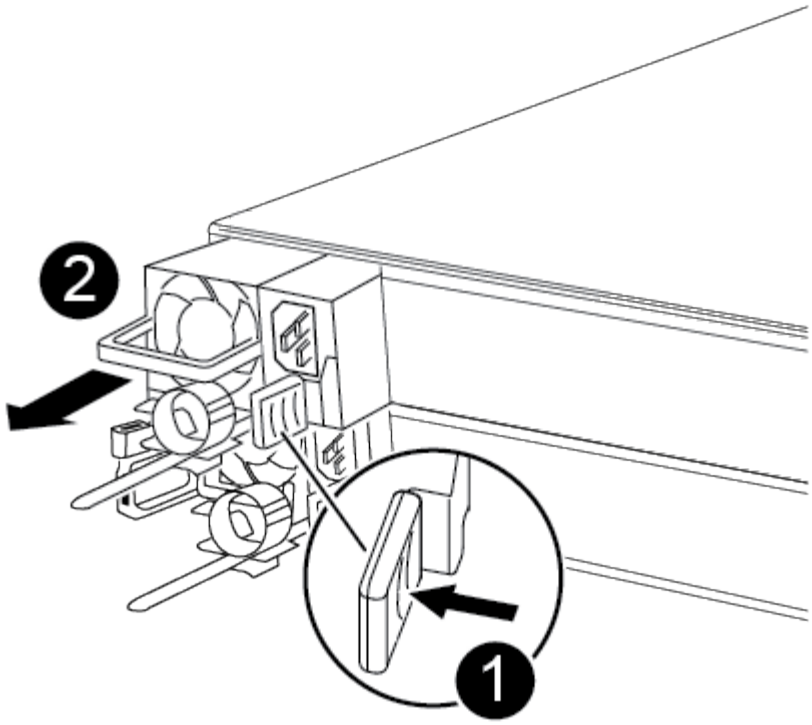


**Step 2: Move the power supply**

You must move the power supply from the impaired controller module to the replacement controller module when you replace a controller module.

1. Disconnect the power supply.
2. Open the power cable retainer, and then unplug the power cable from the power supply.
3. Unplug the power cable from the power source.
4. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

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




| | |
|---|---|
| 1 | Blue power supply locking tab |
| 2 | Power supply |

5. Move the power supply to the new controller module, and then install it.
6. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

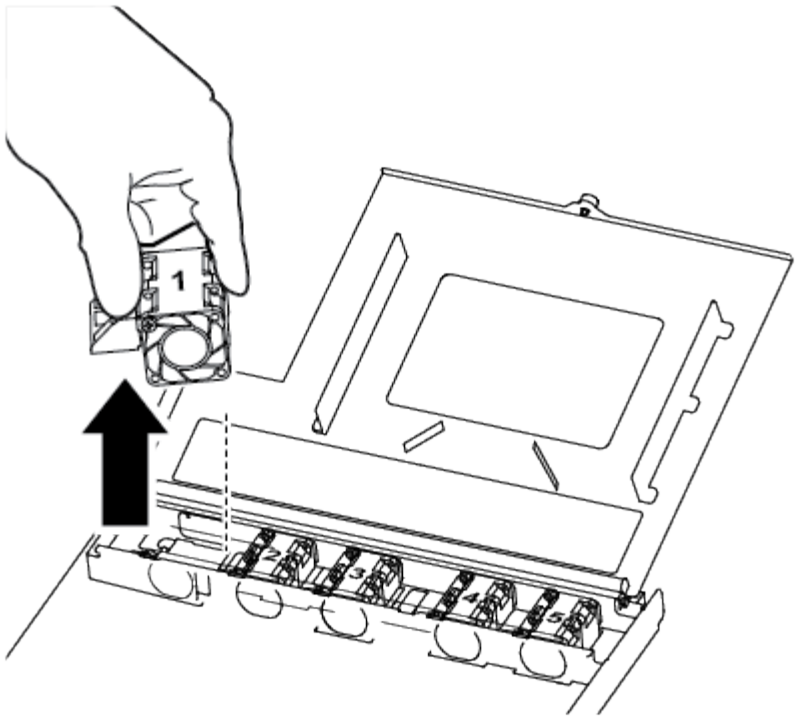
   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

**Step 3: Move the fans**

## You must move the fans from the impaired controller module to the replacement module when replacing a failed controller module.

1. Remove the fan module by pinching the side of the fan module, and then lifting the fan module straight out of the controller module.




| | |
|---|---|
| 1 | Fan module |

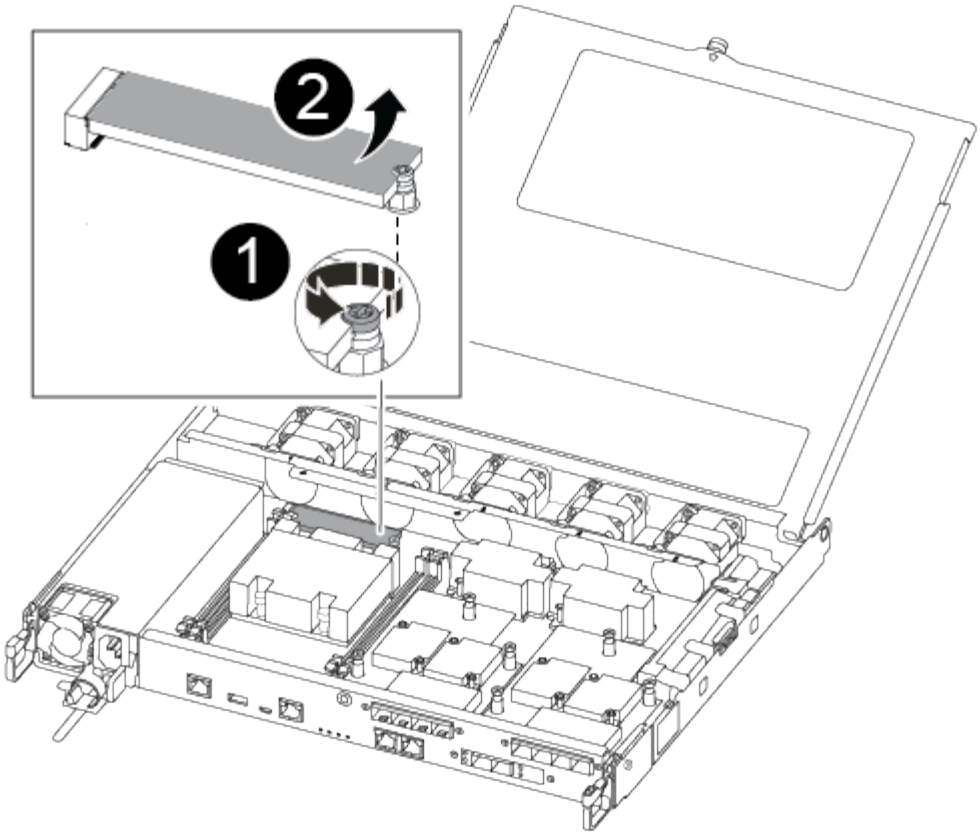
2. Move the fan module to the replacement controller module, and align the edges of the fan module with the opening in the controller module, and then slide the fan module in.
3. Repeat these steps for the remaining fan modules.

**Step 4: Move the boot media**

## There is one boot media device in the AFF A250 under the air duct in the controller module. You must move it from the impaired controller module to the replacement controller module.

You need a #1 magnetic Phillips head screwdriver to remove the screw that holds the boot media in place. Due to the space constraints within the controller module, you should also have a magnet to transfer the screw on to so that you do not lose it.

1. Locate and move the boot media from the impaired controller module to the replacement controller module.



| | |
|---|---|
| 1 | Remove the screw securing the boot media to the motherboard in the impaired controller module. |
| 2 | Lift the boot media out of the impaired controller module. |

a. Using the #1 magnetic screwdriver, remove the screw from the boot media, and set it aside safely on the magnet.
b. Gently lift the boot media directly out of the socket and align it into place in the replacement controller module.
c. Using the #1 magnetic screwdriver, insert and tighten the screw on the boot media.

> Do not apply force when tightening the screw on the boot media; you might crack it.

**Step 5: Move the DIMMs**

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

+
image::../media/drw_a250_dimm_replace.png[]

+
IMPORTANT: Install each DIMM into the same slot it occupied in the impaired controller module.

1. Slowly push apart the DIMM ejector tabs on either side of the DIMM, and slide the DIMM out of the slot.

> Hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

2. Locate the corresponding DIMM slot on the replacement controller module.
3. Make sure that the DIMM ejector tabs on the DIMM socket are in the open position, and then insert the DIMM squarely into the socket.

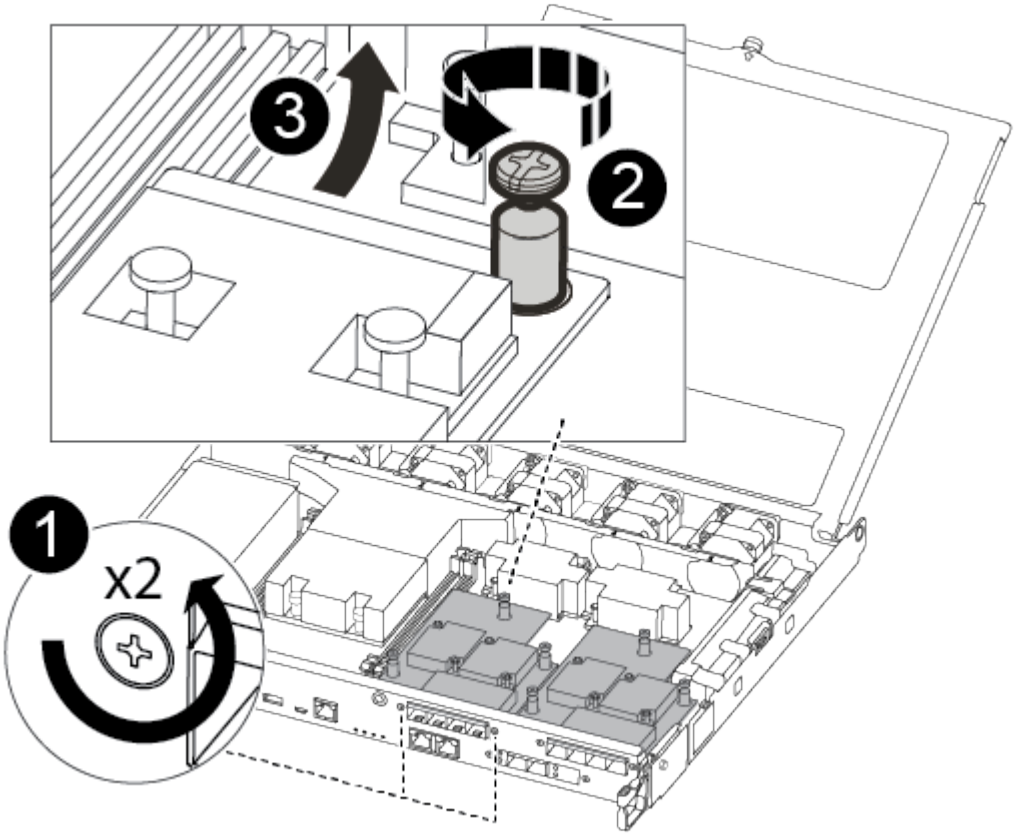
   The DIMMs fit tightly in the socket. If not, reinsert the DIMM to realign it with the socket.

4. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.
5. Repeat these steps for the remaining DIMM.

**Step 6: Move a mezzanine card**

To move a mezzanine card, you must remove the cabling and any QSFPs and SFPs from the ports, move the mezzanine card to the replacement controller, reinstall any QSFPs and SFPs onto the ports, and cable the ports.

1. Locate and move the mezzanine cards from your impaired controller module.




| | |
|---|---|
| 1 | Remove screws on the face of the controller module. |

| | |
|---|---|
| ❷ | Loosen the screw in the controller module. |
| ❸ | Move the mezzanine card. |

2. Unplug any cabling associated with the mezzanine card.

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

   a. Remove any SFP or QSFP modules that might be in the mezzanine card and set it aside.
   b. Using the #1 magnetic screwdriver, remove the screws from the face of the impaired controller module and from the mezzanine card, and set them aside safely on the magnet.
   c. Gently lift the mezzanine card out of the socket and move it to the same position in the replacement controller.
   d. Gently align the mezzanine card into place in the replacement controller.
   e. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the replacement controller module and on the mezzanine card.

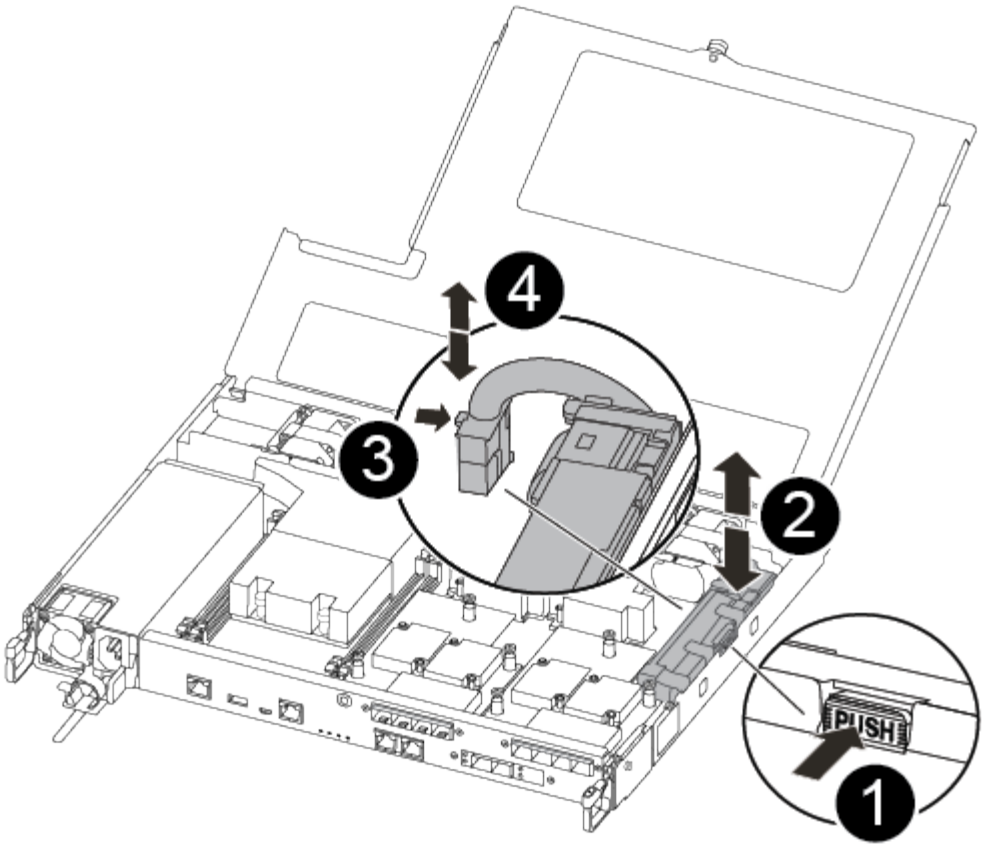
   > Do not apply force when tightening the screw on the mezzanine card; you might crack it.

3. Repeat these steps if there is another mezzanine card in the impaired controller module.
4. Insert the SFP or QSFP modules that were removed onto the mezzanine card.

**Step 7: Move the NV battery**

When replacing the controller module, you must move the NV battery from the impaired controller module to the replacement controller module.

1. Locate and move the NVMEM battery from your impaired controller module to the replacement controller module.




| | |
|---|---|
| 1 | Squeeze the clip on the face of the battery plug. |
| 2 | Unplug the battery cable from the socket. |
| 3 | Grasp the battery and press the blue locking tab marked PUSH. |
| 4 | Lift the battery out of the holder and controller module. |

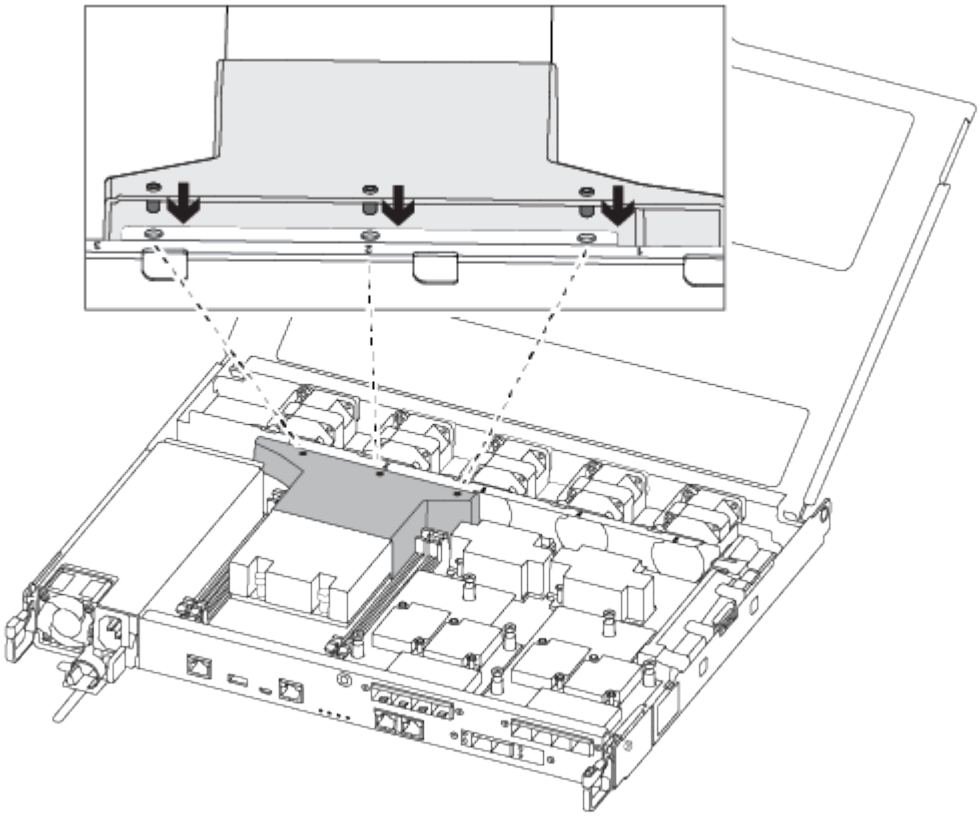
2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Locate the corresponding NV battery holder on the replacement controller module and align the NV battery to the battery holder.
5. Insert the NV battery plug into the socket.
6. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
7. Press firmly down on the battery pack to make sure that it is locked into place.

**Step 8: Install the controller module**

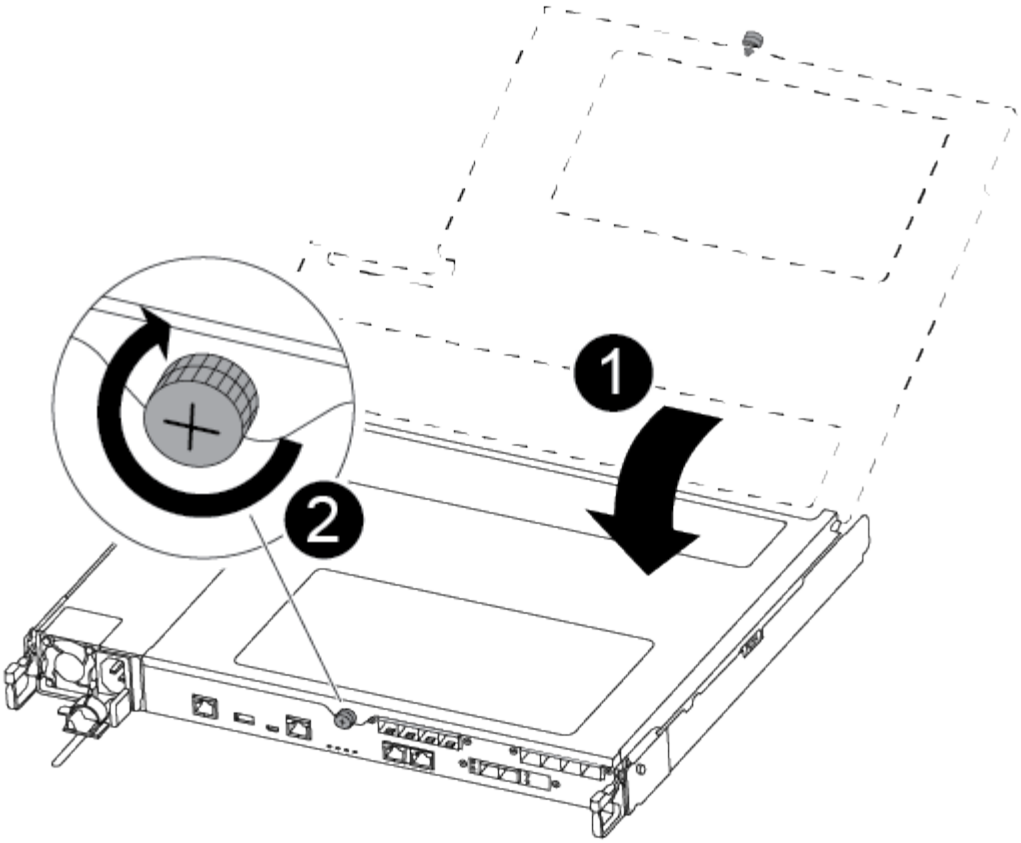
After all of the components have been moved from the impaired controller module to the replacement controller module, you must install the replacement controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustration or the written steps to install the replacement controller module in the chassis.

1. If you have not already done so, install the air duct.



2. Close the controller module cover and tighten the thumbscrew.



| | |
|---|---|
| 1 | Controller module cover |
| 2 | Thumbscrew |

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. Insert the controller module into the chassis.
6. Ensure the latching mechanism arms are locked in the fully extended position.
7. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
8. Place your index fingers through the finger holes from the inside of the latching mechanism.
9. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
10. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching

mechanisms snap into place.

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

The controller module should be fully inserted and flush with the edges of the chassis.

#### Restore and verify the system configuration - FAS500f

## 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 after replacing the controller

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

#### About this task

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

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

#### Steps

1. 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: `show date`

   The date and time are given in GMT.

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 HA state of the chassis

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

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

The HA state should be the same for all components.

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

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

   - ha
   - mcc
   - mccip
   - non-ha

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

**Step 3: Run diagnostics**

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test System** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

     During the boot process, you might see the following prompts:

     - A prompt warning of a system ID mismatch and asking to override the system ID.
     - A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
       You can safely respond `y` to these prompts.

#### Recable the system and reassign disks - FAS500f

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

### Step 1: Recable the system

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

#### Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

### Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must confirm the system ID change when you boot the *replacement* controller and then verify that the change was implemented.

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

1. If the *replacement* controller 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* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, 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 controller, 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`
                                    Takeover
Node              Partner           Possible     State Description
------------      ------------      --------
-------------------------------------
node1             node2             false        System ID changed on
partner (Old:
                                                 151759755, New:
151759706), In takeover
node2             node1             -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, 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 controller:

   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode replacement_node_name`

      The *replacement* controller 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 content 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* controller 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 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. If the system is in a MetroCluster configuration, monitor the status of the controller: `metrocluster node`

`show`

The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each controller 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 controller 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 controller on the disaster site.

   This is required if both of the following are true:

   - The MetroCluster configuration is in a switchover state.
   - The *replacement* controller 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 controller 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 controller: `vol show -node node-name`
11. If you disabled automatic takeover on reboot, enable it from the healthy controller: `storage failover modify -node replacement-node-name -onreboot true`

#### Complete system restoration - FAS500f

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

### Step 1: Install licenses for the replacement controller in ONTAP

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

#### About this task

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

#### Before you begin

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.

#### 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: Restore Storage and Volume Encryption functionality

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

#### Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use 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

### Step 3: Verify LIFs and registering the serial number

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

#### Steps

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

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

2. Register the system serial number with NetApp Support.
   - 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. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

#### 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 & Replacements page for further information.

### Replace a DIMM - FAS500f

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

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

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

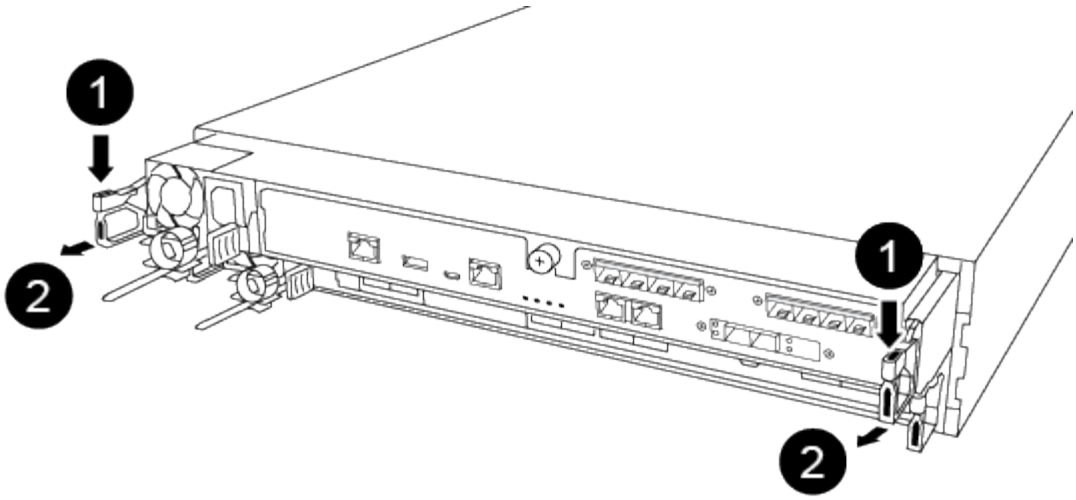
#### Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

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

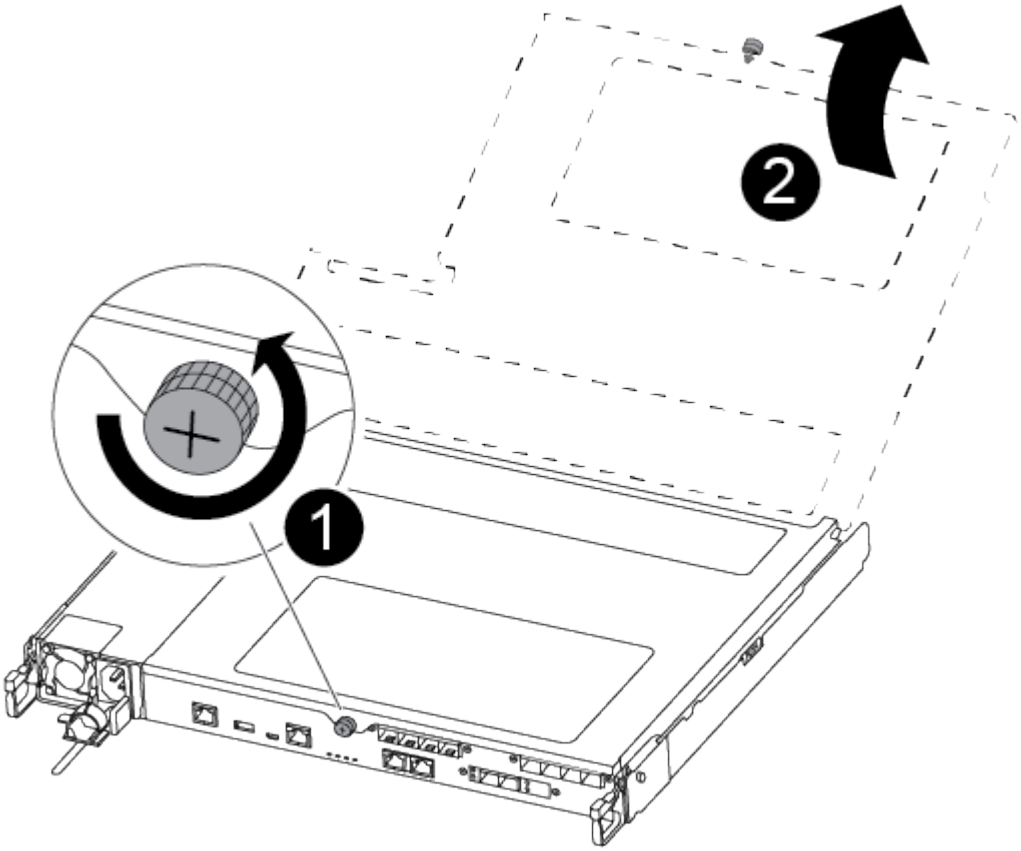
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



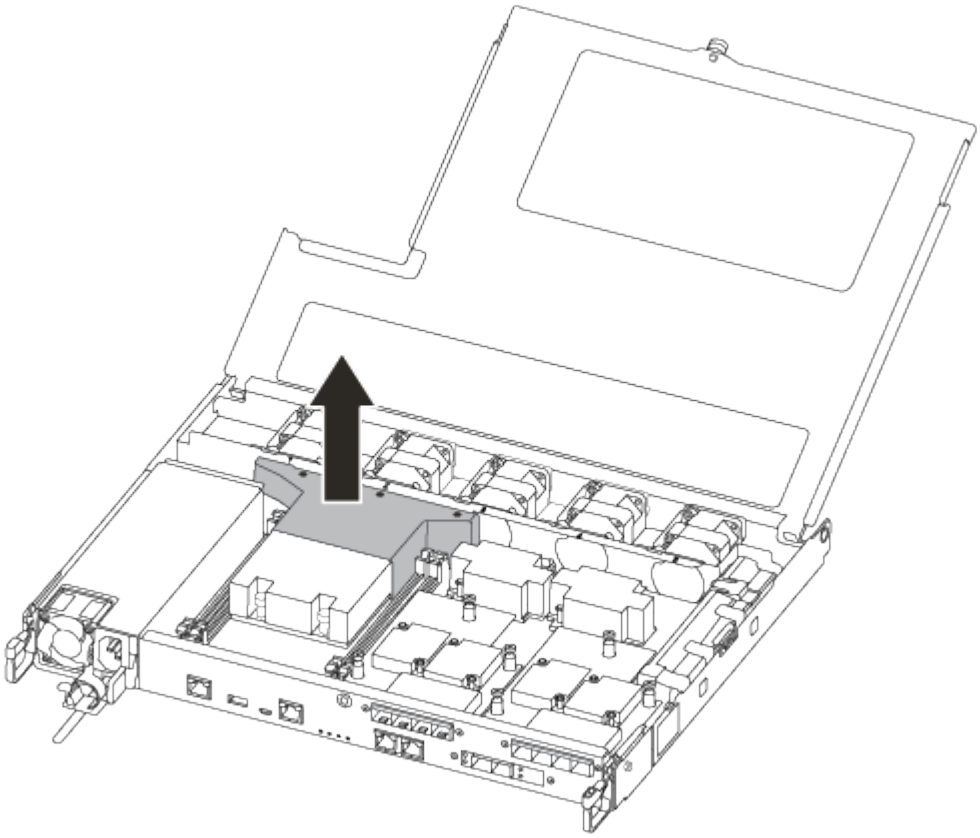
| | |
|---|---|
| 1 | Lever |
| 2 | Latching mechanism |

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.



| | |
|---|---|
| ❶ | Thumbscrew |
| ❷ | Controller module cover. |

7. Lift out the air duct cover.



**Step 3: Replace a DIMM**

To replace a DIMM, you must locate it in the controller module using the DIMM map label on top of the air duct or locating it using the LED next to the DIMM, and then replace it following the specific sequence of steps.

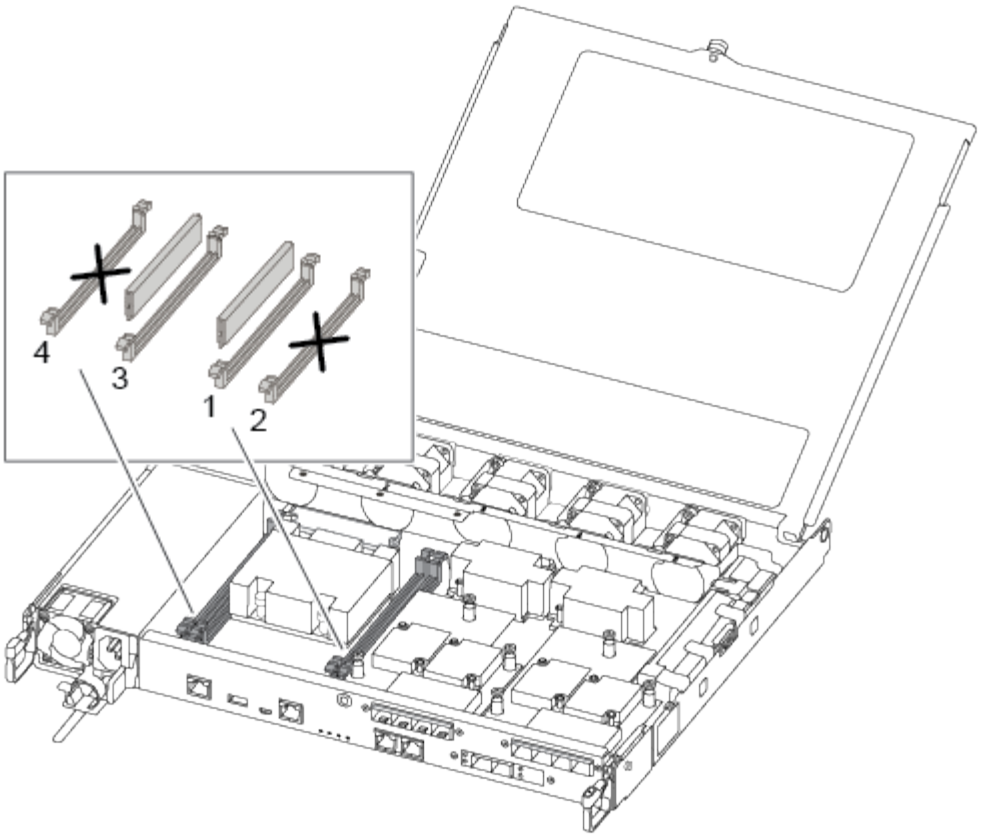
You can use the following video or the tabulated steps to replace a DIMM:

Replacing a DIMM

1. Replace the impaired DIMM on your controller module.

   The DIMMs are in slot 3 or 1 on the motherboard. Slot 2 and 4 are left empty. Do not attempt to install DIMMs into these slots.

   ⓘ The fault LED located on the board next to each DIMM blinks every two seconds.




2. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
3. Slowly push apart the DIMM ejector tabs on either side of the DIMM, and slide the DIMM out of the slot.
4. Leave DIMM ejector tabs on the connector in the open position.
5. Remove the replacement DIMM from the antistatic shipping bag, hold the DIMM by the corners, and align it to the slot.

   > Hold the DIMM by the edges to avoid pressure on the components on the DIMM circuit board.

6. Insert the replacement DIMM squarely into the slot.

   The DIMMs fit tightly in the socket. If not, reinsert the DIMM to realign it with the socket.

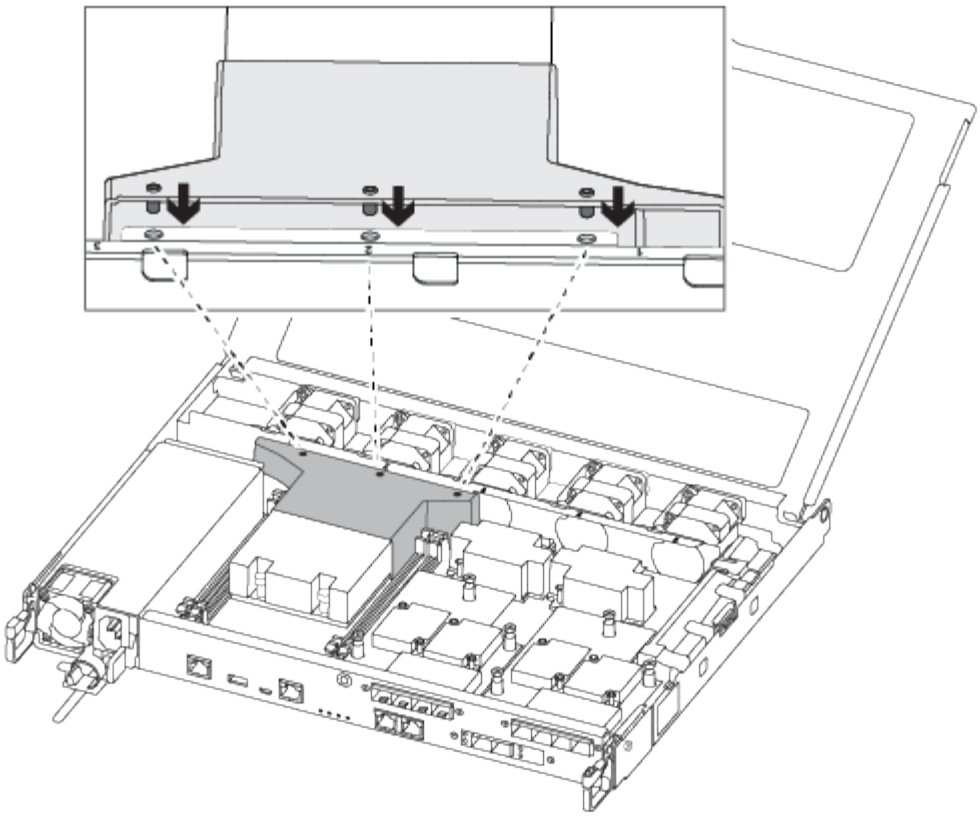
7. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.

#### Step 4: Install the controller module

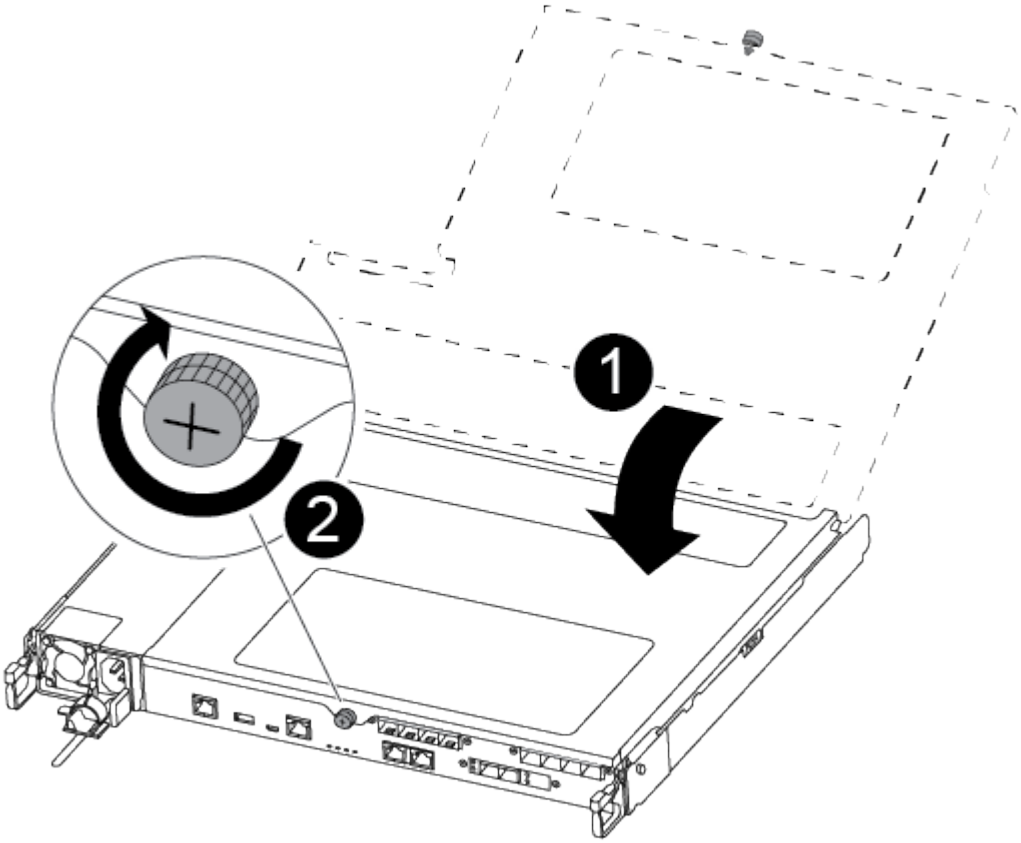
After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustration or the written steps to install the replacement controller module in the chassis.

1. If you have not already done so, install the air duct.



2. Close the controller module cover and tighten the thumbscrew.



| | |
|---|---|
| ❶ | Controller module cover |
| ❷ | Thumbscrew |

3. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
   c. Place your index fingers through the finger holes from the inside of the latching mechanism.
   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

   The controller module should be fully inserted and flush with the edges of the chassis.

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.

#### Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

#### 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 & Replacements page for further information.

### Replace SSD Drive or HDD Drive - AFF C190

You can replace a failed drive nondisruptively while I/O is in progress. The procedure for replacing an SSD is meant for non-spinning drives and the procedure for replacing an HDD is meant for spinning drives.

When a drive fails, the platform logs a warning message to the system console indicating which drive has failed. In addition, both the fault LED on the operator display panel and the fault LED on the failed drive are illuminated.

#### Before you begin

- Follow best practice and install the current version of the Disk Qualification Package (DQP) before replacing a drive.
- Identify the failed disk drive by running the `storage disk show -broken` command from the system console.

  The failed drive appears in the list of failed drives. If it does not, you should wait, and then run the command again.

  > Depending on the drive type and capacity, it can take up to several hours for the drive to appear in the list of failed drives.

- Determine whether SED authentication is enabled.

  How you replace the disk depends on how the disk drive is being used. If SED authentication is enabled, you must use the SED replacement instructions in the ONTAP 9 NetApp Encryption Power Guide. These Instructions describe additional steps you must perform before and after replacing an SED.

- Make sure the replacement drive is supported by your platform. See the NetApp Hardware Universe.
- Make sure all other components in the system are functioning properly; if not, you must contact technical support.

#### About this task

Drive firmware is automatically updated (nondisruptively) on new drives that have non current firmware versions.

When replacing several disk drives, you must wait one minute between the removal of each failed disk drive and the insertion of the replacement disk drive to allow the storage system to recognize the existence of each new disk.

#### Procedure

Replace the failed drive by selecting the option appropriate to the drives that your platform supports.

You may also choose to watch the Replace failed drive video that shows an overview of the embedded drive replacement procedure.

**Option 1: Replace SSD**

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Physically identify the failed drive.

   When a drive fails, the system logs a warning message to the system console indicating which drive failed. Additionally, the attention (amber) LED on the drive shelf operator display panel and the failed drive illuminate.

   > The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.

4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.

6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

7. Verify that the drive’s activity (green) LED is illuminated.

   When the drive’s activity LED is solid, it means that the drive has power. When the drive’s activity LED

is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

8. If you are replacing another drive, repeat Steps 3 through 7.
9. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
   a. Display all unowned drives: `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

      You can enter the command on either controller module.

      You can use the wildcard character to assign more than one drive at once.

   c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.

10. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

**Option 2: Replace HDD**

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the failed disk drive from the system console warning message and the illuminated fault LED on the disk drive
5. Press the release button on the disk drive face.

Depending on the storage system, the disk drives have the release button located at the top or on the left of the disk drive face.

For example, the following illustration shows a disk drive with the release button located on the top of the disk drive face:

The cam handle on the disk drive springs open partially and the disk drive releases from the midplane.

6. Pull the cam handle to its fully open position to unseat the disk drive from the midplane.

7. Slide out the disk drive slightly and allow the disk to safely spin down, which can take less than one minute, and then, using both hands, remove the disk drive from the disk shelf.
8. With the cam handle in the open position, insert the replacement disk drive into the drive bay, firmly pushing until the disk drive stops.

   Wait a minimum of 10 seconds before inserting a new disk drive. This allows the system to recognize that a disk drive was removed.

   If your platform drive bays are not fully loaded with drives, it is important to place the replacement drive into the same drive bay from which you removed the failed drive.

   Use two hands when inserting the disk drive, but do not place hands on the disk drive boards that are exposed on the underside of the disk carrier.

9. Close the cam handle so that the disk drive is fully seated into the midplane and the handle clicks into place.

   Be sure to close the cam handle slowly so that it aligns correctly with the face of the disk drive..

10. If you are replacing another disk drive, repeat Steps 4 through 9.
11. Reinstall the bezel.
12. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
    a. Display all unowned drives: `storage disk show -container-type unassigned`

       You can enter the command on either controller module.

    b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

       You can enter the command on either controller module.

       You can use the wildcard character to assign more than one drive at once.

    c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

       You must reenable automatic drive assignment on both controller modules.

13. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

### Replace a fan — FAS500f

## You replace a fan with a new fan module when it fails.

#### Step 1: Shut down the impaired controller

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |

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

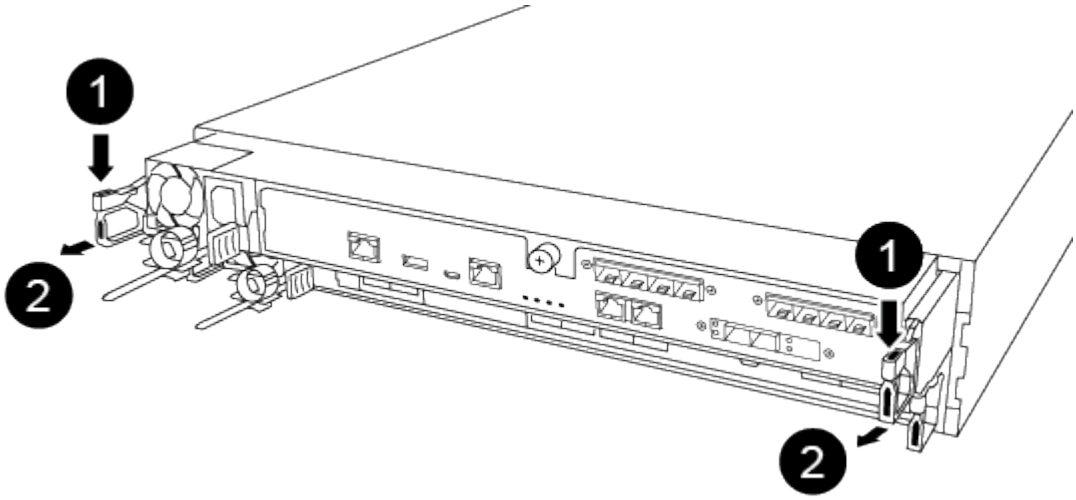
#### Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a fan module.

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

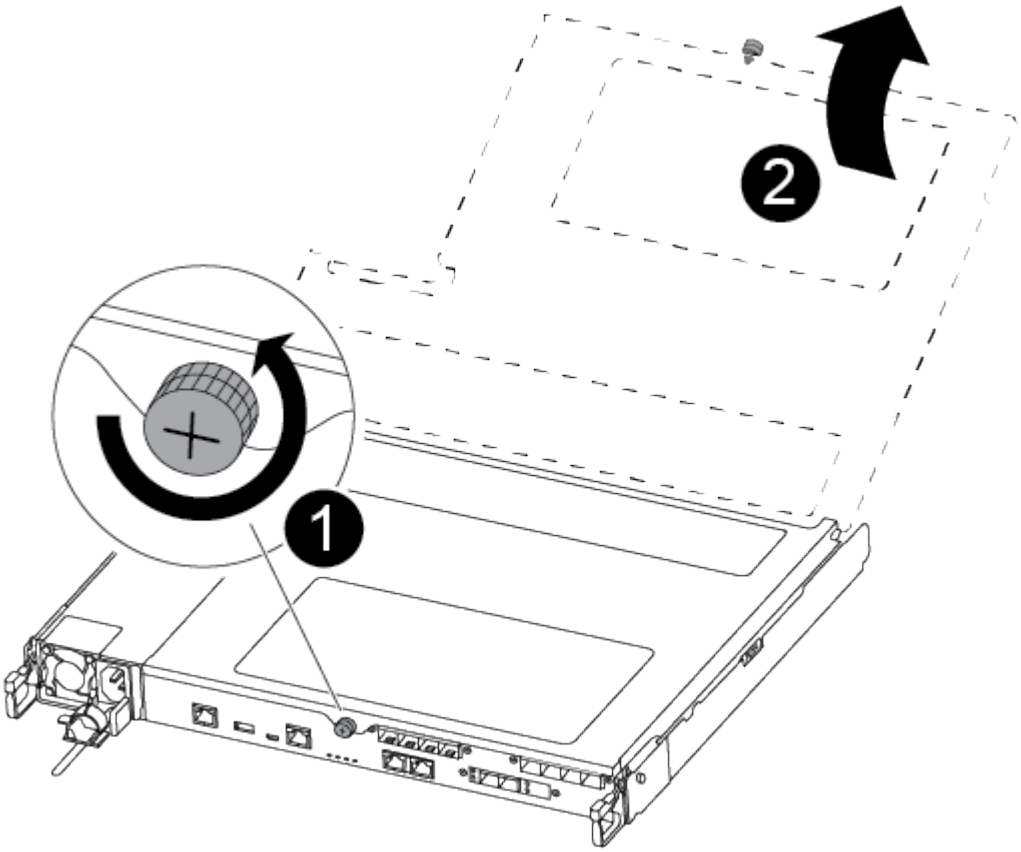
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).




| | |
| --- | --- |
| 1 | Lever |
| 2 | Latching mechanism |

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.




| | |
|---|---|
| 1 | Thumbscrew |
| 2 | Controller module cover |

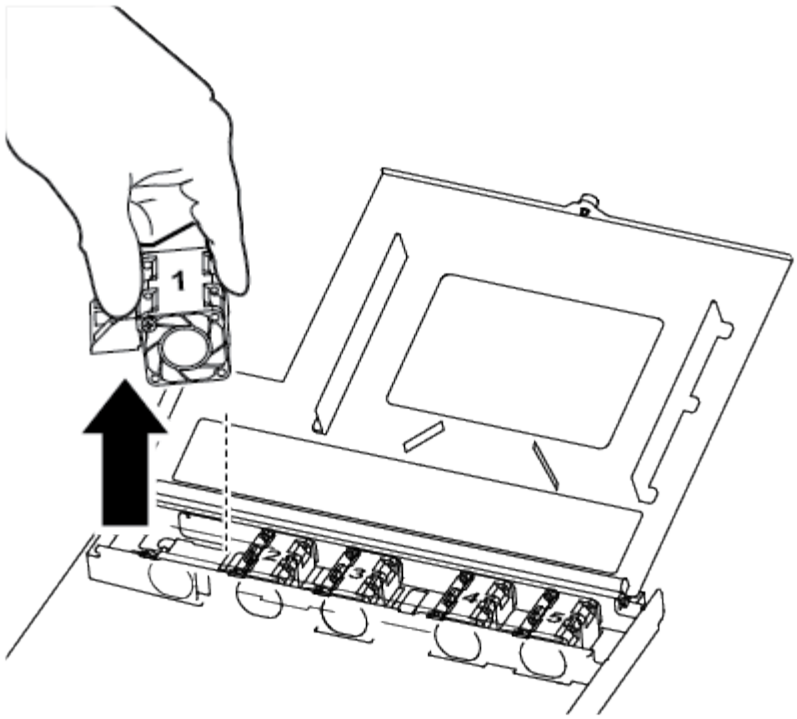
**Step 3: Replace a fan**

To replace a fan, remove the failed fan module and replace it with a new fan module.

You can use the following video or the tabulated steps to replace a fan:

Replacing a fan

1. Identify the fan module that you must replace by checking the console error messages or by locating the lit LED for the fan module on the motherboard.
2. Remove the fan module by pinching the side of the fan module, and then lifting the fan module straight out of the controller module.



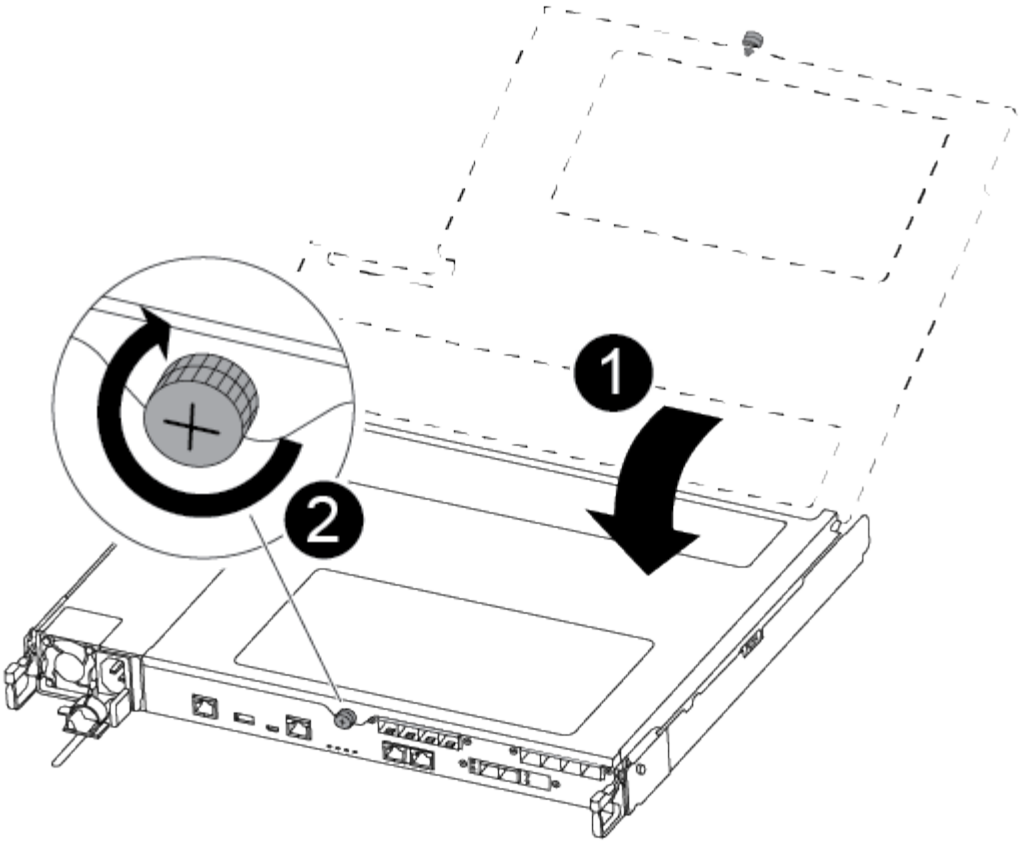

| | |
|---|---|
| 1 | Fan module |

3. Align the edges of the replacement fan module with the opening in the controller module, and then slide the replacement fan module into the controller module.

#### Step 4: Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. Close the controller module cover and tighten the thumbscrew.




| | |
|---|---|
| 1 | Controller module cover |
| 2 | Thumbscrew |

2. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

   The controller module should be fully inserted and flush with the edges of the chassis.

3. Recable the system, as needed.

4. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

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

#### 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 & Replacements page for further information.

### Replace or install a mezzanine card - FAS500f

To replace a failed mezzanine card, you must remove the cables and any SFP or QSFP modules, replace the card, reinstall the SFP or QSFP modules and recable the cards. To install a new mezzanine card, you must have the appropriate cables and SFP or QSFP modules.

- 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

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

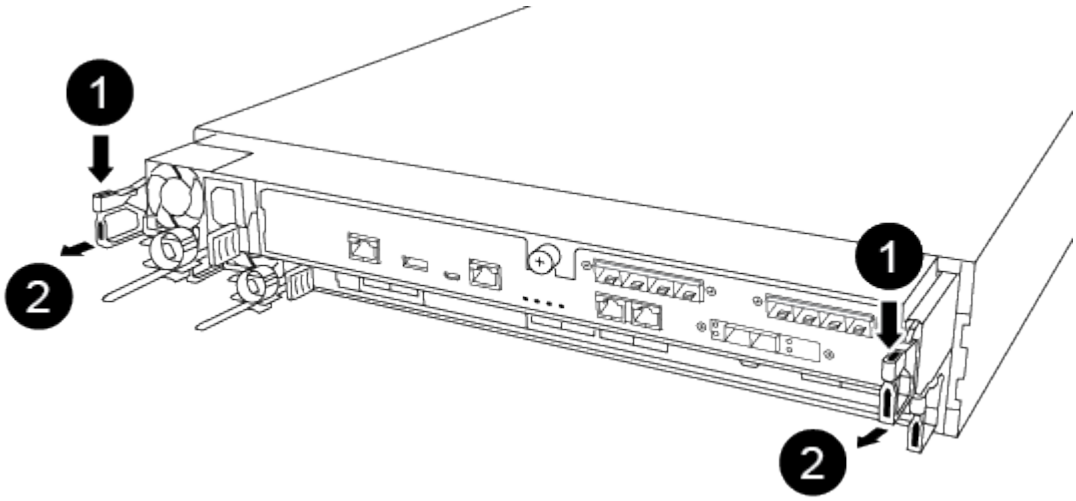
#### Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

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

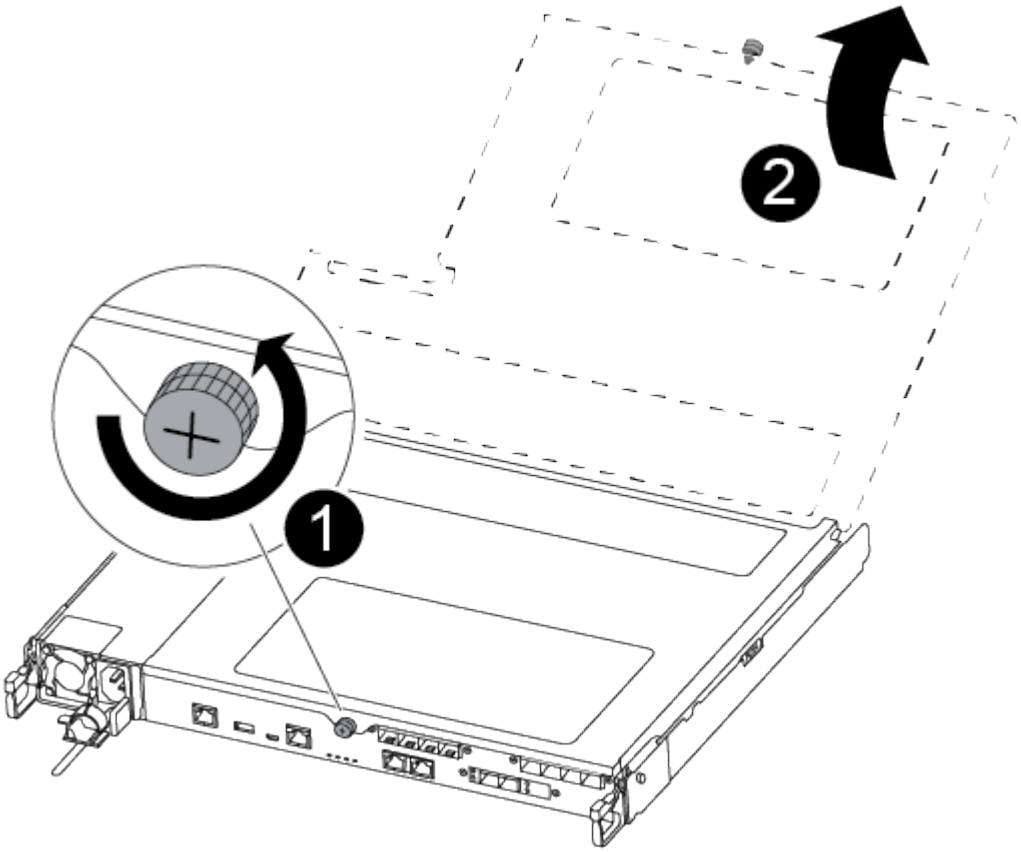
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



| | |
|---|---|
| ❶ | Lever |
| ❷ | Latching mechanism |

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.




| | |
|---|---|
| ❶ | Thumbscrew |
| ❷ | Controller module cover. |

**Step 3: Replace or install a mezzanine card**

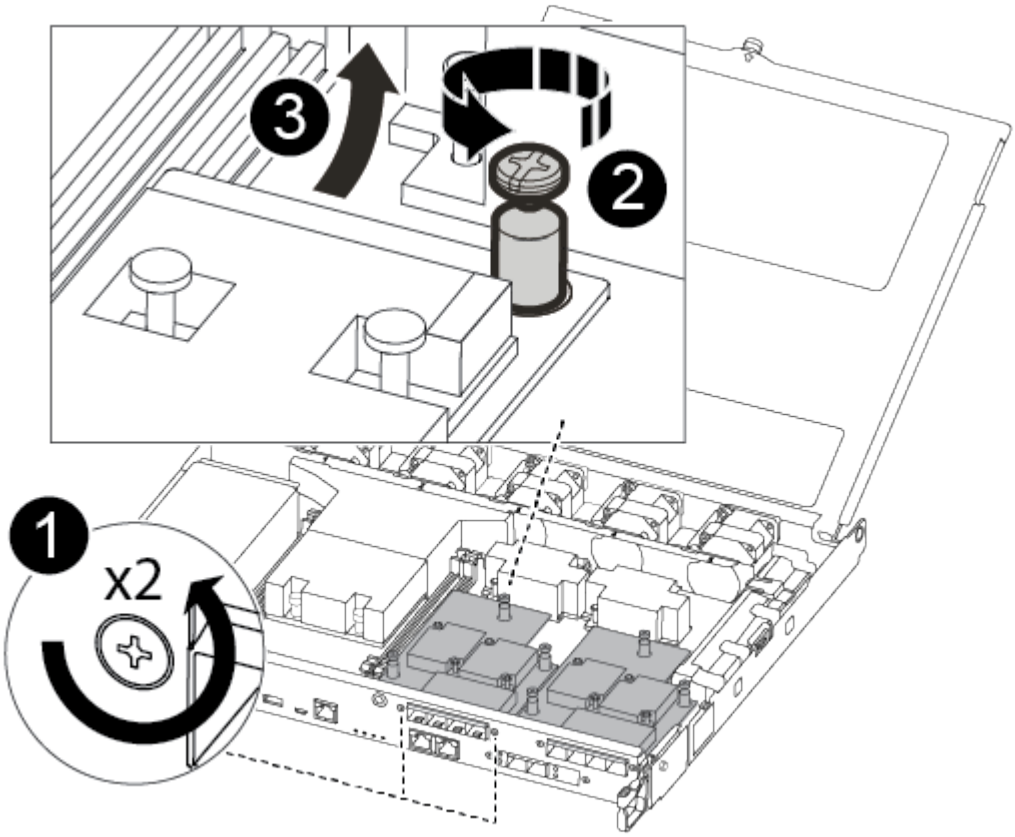
To replace a mezzanine card, you must remove the impaired card and install the replacement card; to install a mezzanine card, you must remove the faceplate and install the new card.

You can use the following video or the tabulated steps to replace a mezzanine card:

Replacing a mezzanine card

**Option 1: Replace a mezzanine card:**

1. Locate and replace the impaired mezzanine card on your controller module.




| | |
|---|---|
| 1 | Remove screws on the face of the controller module. |
| 2 | Loosen the screw in the controller module. |
| 3 | Remove the mezzanine card. |

2. Unplug any cabling associated with the impaired mezzanine card.

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

3. Remove any SFP or QSFP modules that might be in the impaired mezzanine card and set it aside.
4. Using the #1 magnetic screwdriver, remove the screws from the face of the controller module and set them aside safely on the magnet.
5. Using the #1 magnetic screwdriver, loosen the screw on the impaired mezzanine card.
6. Using the #1 magnetic screwdriver, gently lift the impaired mezzanine card directly out of the socket and set it aside.
7. Remove the replacement mezzanine card from the antistatic shipping bag and align it to the inside face of the controller module.
8. Gently align the replacement mezzanine card into place.

9. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the controller module and on the mezzanine card.

> Do not apply force when tightening the screw on the mezzanine card; you might crack it.

10. Insert any SFP or QSFP modules that were removed from the impaired mezzanine card to the replacement mezzanine card.

**Option 2: Install a mezzanine card:**

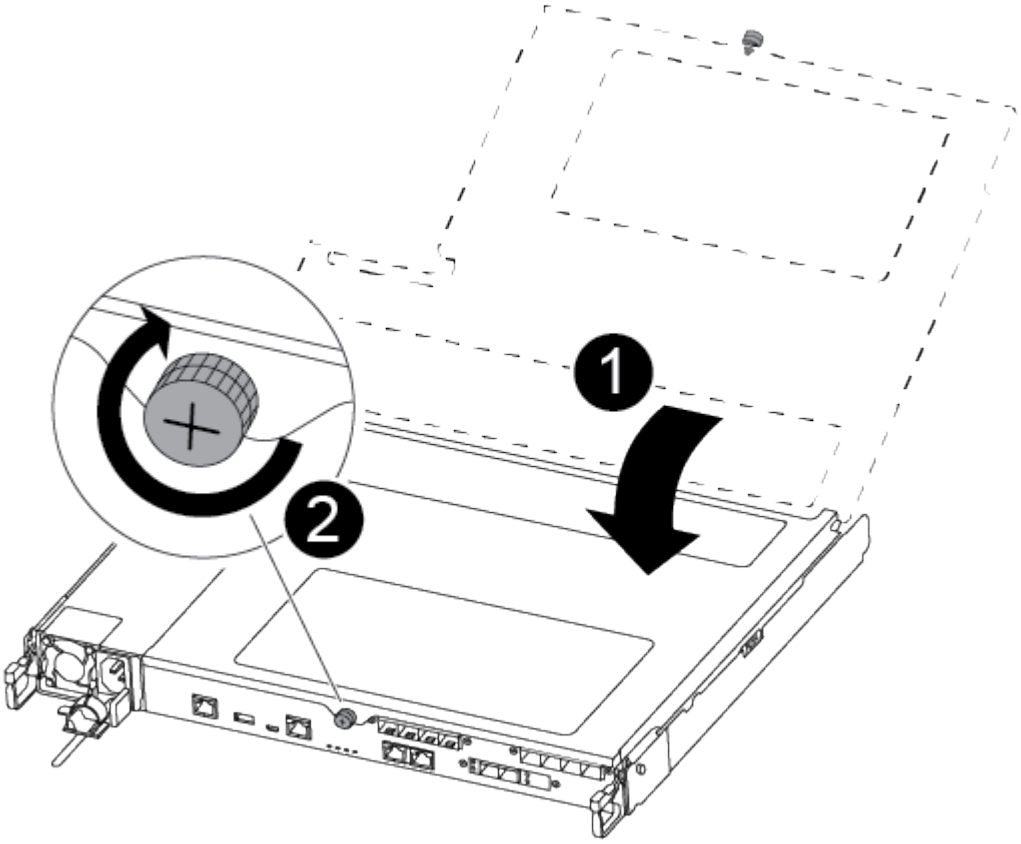
You install a new mezzanine card if your system does not have one.
. Using the #1 magnetic screwdriver, remove the screws from the face of the controller module and the faceplate covering the mezzanine card slot, and set them aside safely on the magnet.
. Remove the mezzanine card from the antistatic shipping bag and align it to the inside face of the controller module.
. Gently align the mezzanine card into place.
. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the controller module and on the mezzanine card.

+
NOTE: Do not apply force when tightening the screw on the mezzanine card; you might crack it.

#### Step 4: Reinstall the controller module

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it.

1. Close the controller module cover and tighten the thumbscrew.



| | |
|---|---|
| ❶ | Controller module cover |
| ❷ | Thumbscrew |

2. Insert the controller module into the chassis

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

   The controller module should be fully inserted and flush with the edges of the chassis.

3. Recable the system, as needed.

4. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

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

#### 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 & Replacements page for further information.

### Replace the NVMEM battery - FAS500f

To replace an NVMEM battery in the system, you must remove the controller module from the system, open it, replace the battery, and close and replace the controller module.

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

#### Step 1: Shut down the impaired controller

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 are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the “Returning SEDs to unprotected mode” section of the *ONTAP 9 NetApp Encryption Power Guide*.

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### Step 2: Remove the controller module

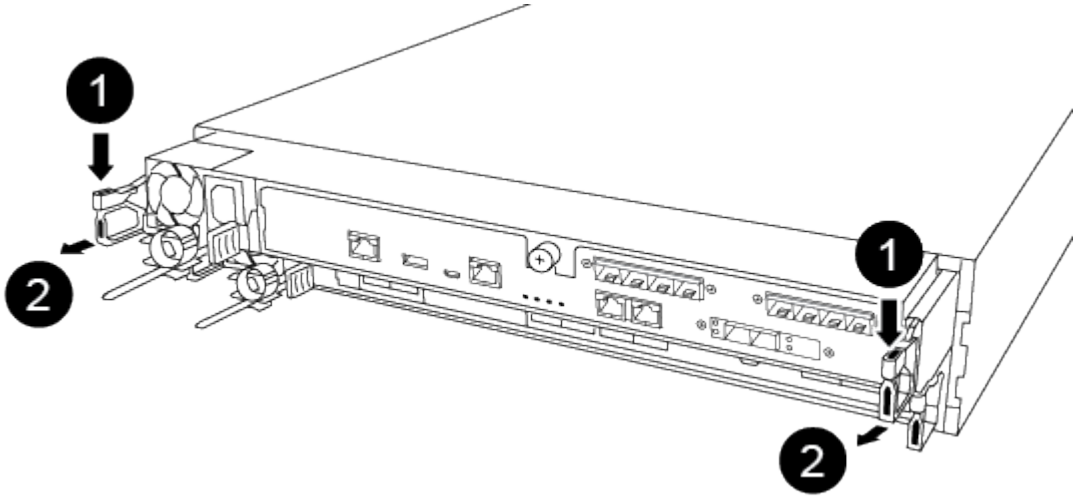
You must remove the controller module from the chassis when you replace a component inside the controller module.

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

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever

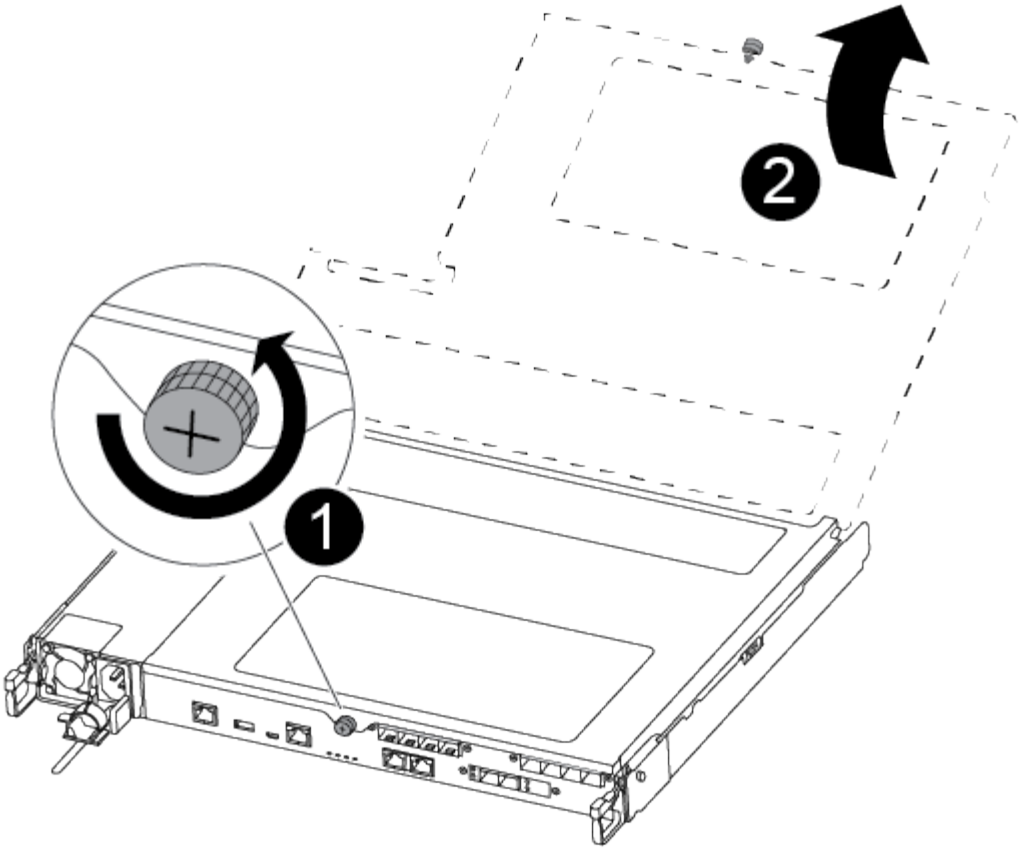
with your thumb, and gently pull the controller a few inches out of the chassis.

> If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).




| | |
|---|---|
| 1 | Lever |
| 2 | Latching mechanism |

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.




| | |
|---|---|
| 1 | Thumbscrew |
| 2 | Controller module cover. |

**Step 3: Replace the NVMEM battery**

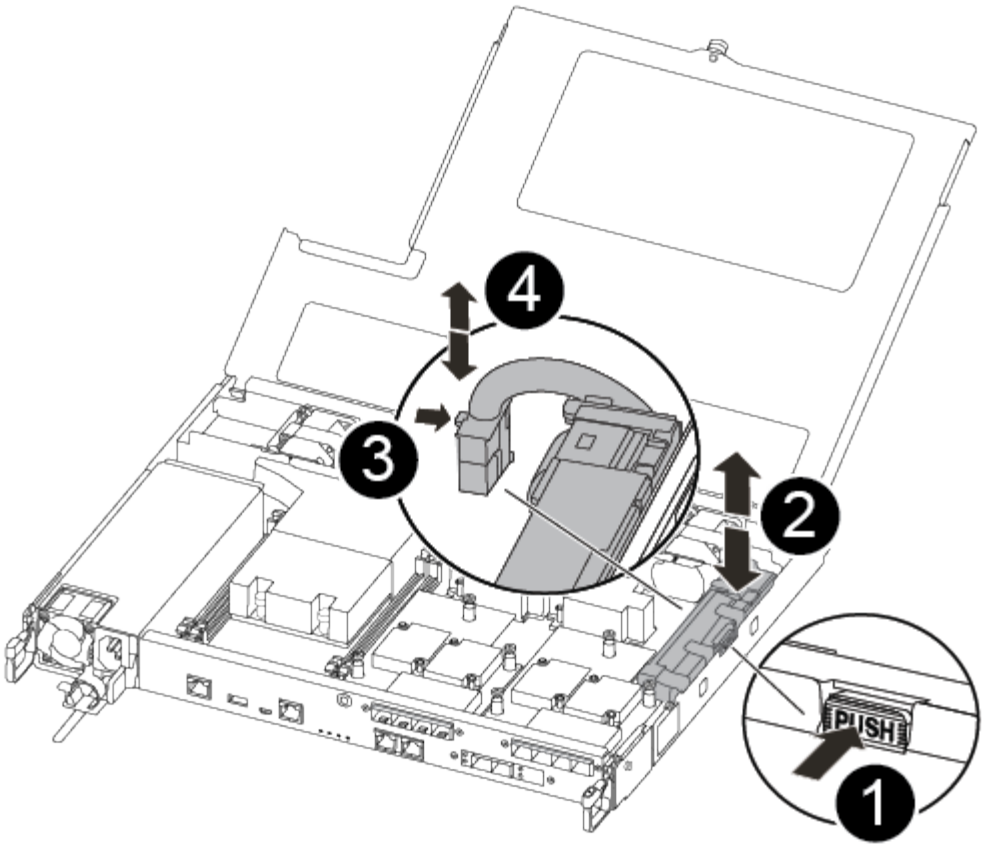
To replace the NVMEM battery, you must remove the failed battery from the controller module and install the replacement battery into the controller module.

You can use the following video or the tabulated steps to replace the NVMEM battery:

Replacing the NVMEM battery

1. Locate and replace the impaired NVMEM battery on your controller module.

> It is recommended that you follow the illustrated instructions in the order listed.




| | |
|---|---|
| 1 | Squeeze the clip on the face of the battery plug. |
| 2 | Unplug the battery cable from the socket. |
| 3 | Grasp the battery and press the blue locking tab marked PUSH. |
| 4 | Lift the battery out of the holder and controller module. |

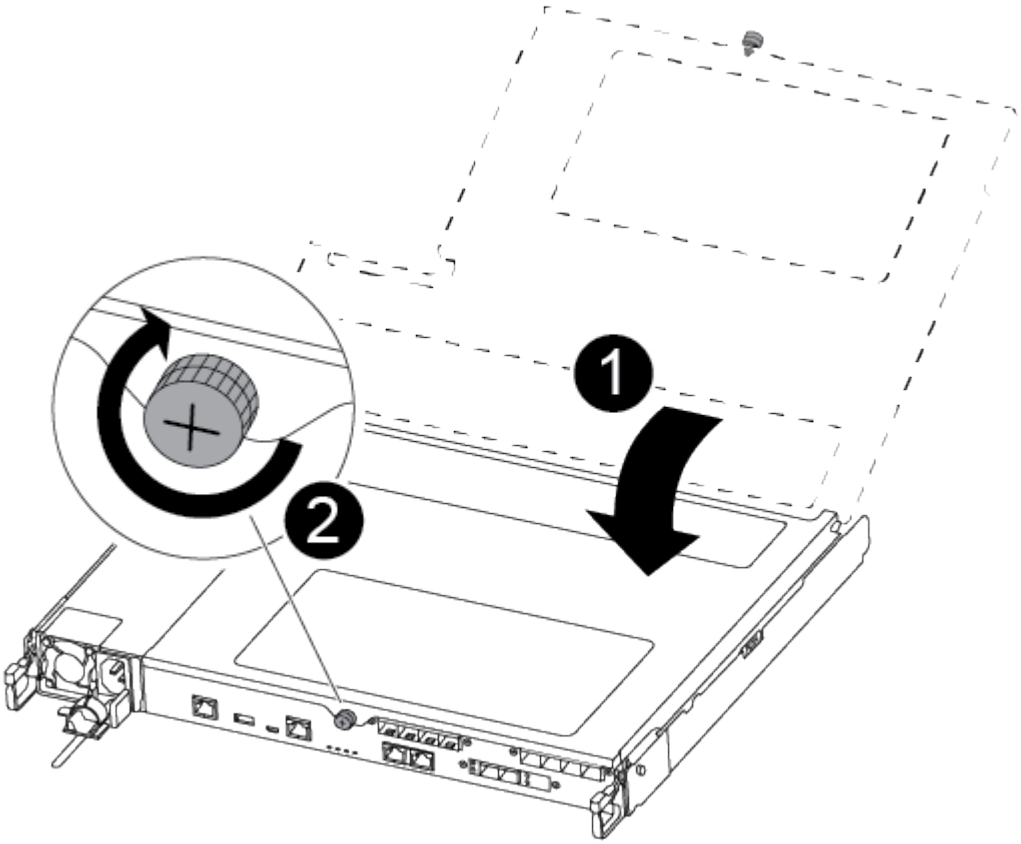
2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module and set it aside.
4. Remove the replacement NV battery from the antistatic shipping bag and align it to the battery holder.
5. Insert the replacement NV battery plug into the socket.
6. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
7. Press firmly down on the battery pack to make sure that it is locked into place.

**Step 4: Install the controller module**

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustration or the written steps to install the replacement controller module in the chassis.

1. Close the controller module cover and tighten the thumbscrew.




| | |
|---|---|
| 1 | Controller module cover |
| 2 | Thumbscrew |

2. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.

   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.

   c. Place your index fingers through the finger holes from the inside of the latching mechanism.

   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.

   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

The controller module should be fully inserted and flush with the edges of the chassis.

3. 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.

#### Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

**Steps**

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test system** from the displayed menu to run diagnostics tests.
5. Proceed based on the result of the preceding step:
   - If the scan show problems, correct the issue, and then rerun the scan.
   - If the scan reported no failures, select Reboot from the menu to reboot the system.

#### 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 & Replacements page for further information.

### Replace a power supply - FAS500f

Replacing a power supply involves disconnecting the target power supply (PSU) from the power source, unplugging the power cable, removing the old PSU and installing the replacement PSU, and then reconnecting it to the power source.

- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

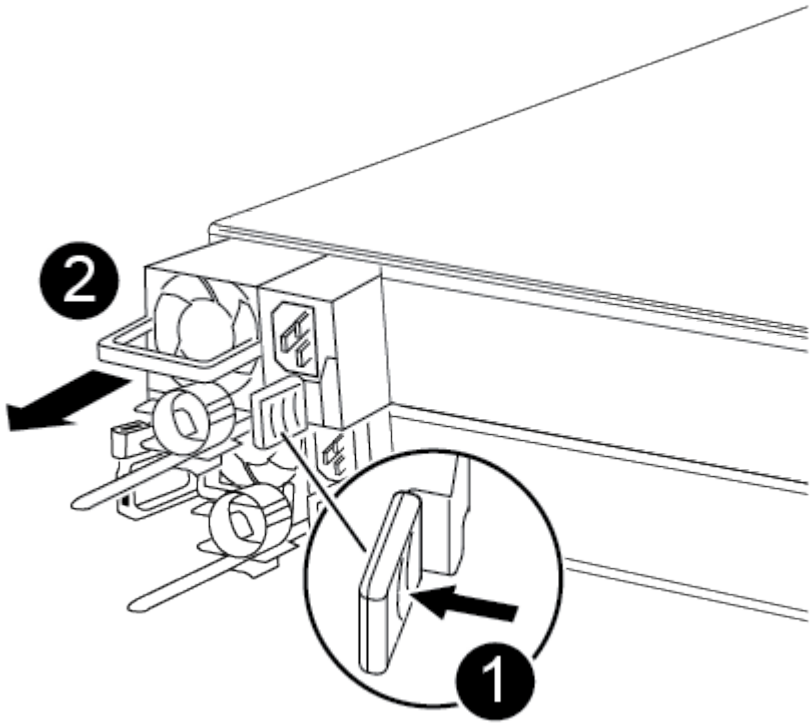
> It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.

You can use the following video or the tabulated steps to replace the power supply:

Replacing the power supply

1. If you are not already grounded, properly ground yourself.
2. Identify the power supply you want to replace, based on console error messages or through the red Fault LED on the power supply.
3. Disconnect the power supply:
   a. Open the power cable retainer, and then unplug the power cable from the power supply.
   b. Unplug the power cable from the power source.
4. Rotate the cam handle such that it can be used to pull power supply out of the controller module while pressing the locking tab.

> The power supply is short. Always use two hands to support it when removing it from the controller module so that it does not suddenly swing free from the controller module and injure you.




| | |
|---|---|
| 1 | Blue power supply locking tab |
| 2 | Power supply |

5. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

6. 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.

7. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Replace the real-time clock battery

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.

#### Step 1: Shut down the impaired controller

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

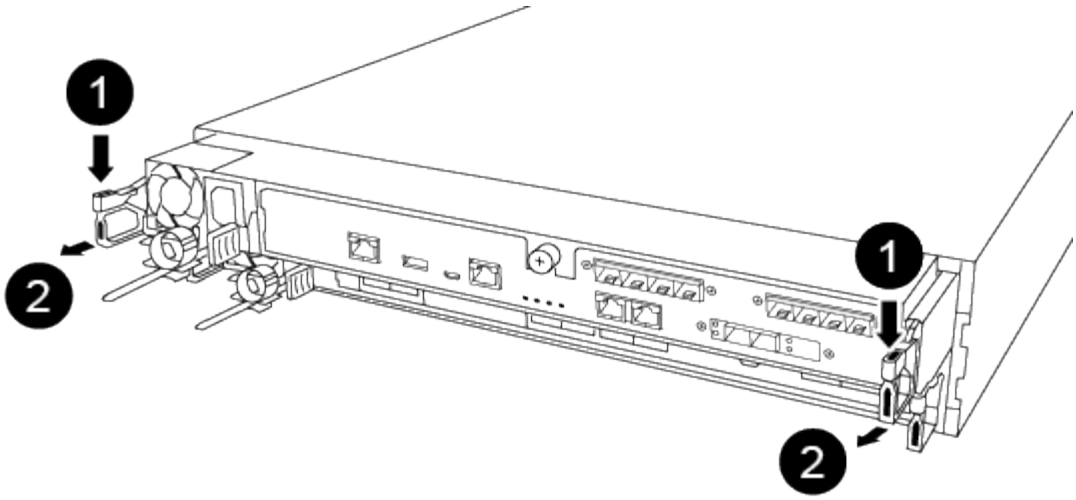
#### Step 2: Remove the controller module

You must remove the controller module from the chassis when you replace a component inside the controller module.

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

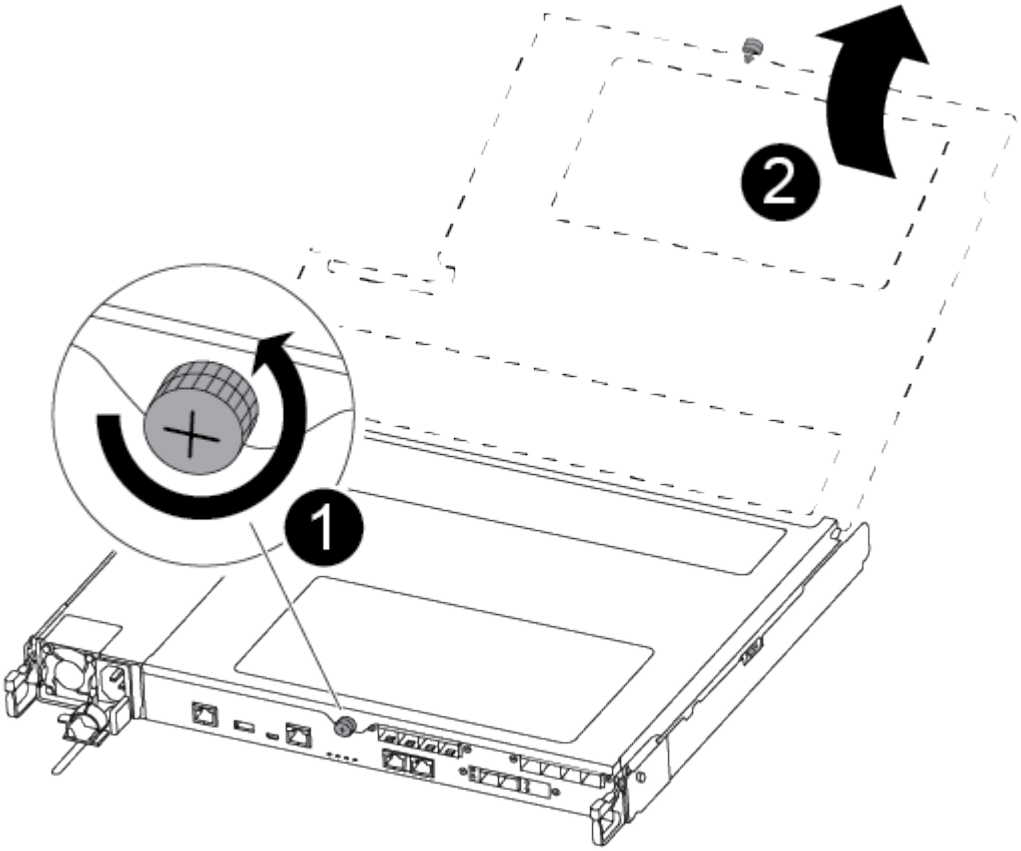
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Insert your forefinger into the latching mechanism on either side of the controller module, press the lever with your thumb, and gently pull the controller a few inches out of the chassis.

   > If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



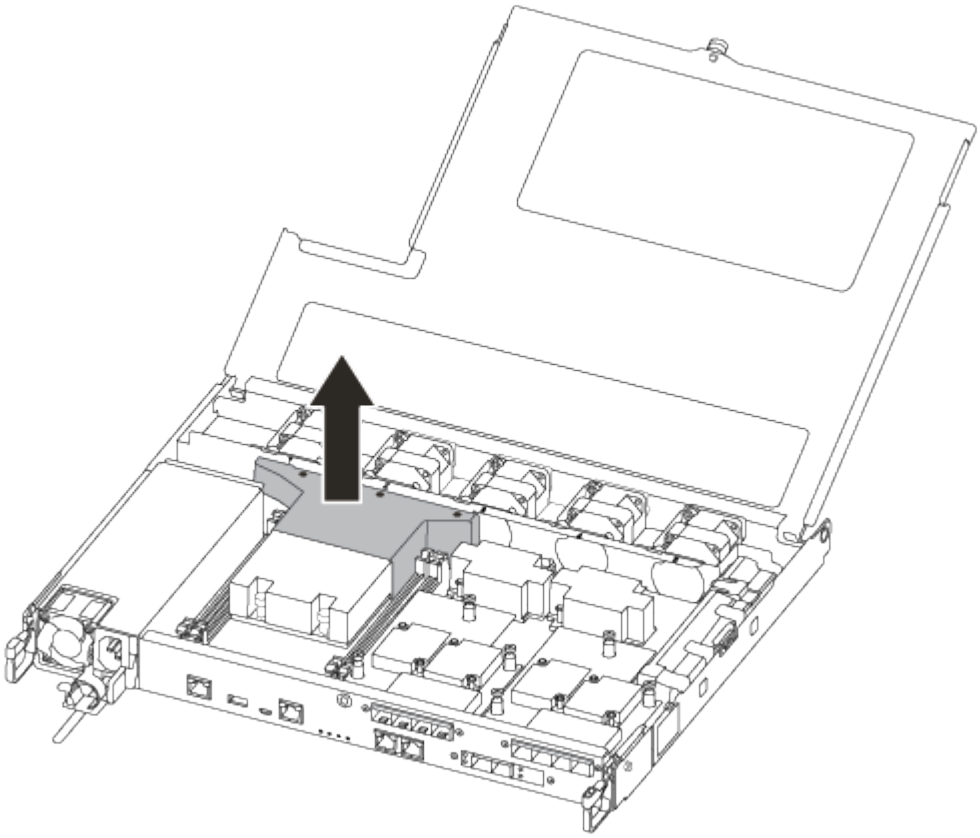

| | |
|---|---|
| 1 | Lever |
| 2 | Latching mechanism |

5. Using both hands, grasp the controller module sides and gently pull it out of the chassis and set it on a flat, stable surface.
6. Turn the thumbscrew on the front of the controller module anti-clockwise and open the controller module cover.



| | |
|---|---|
| ❶ | Thumbscrew |
| ❷ | Controller module cover. |

7. Lift out the air duct cover.



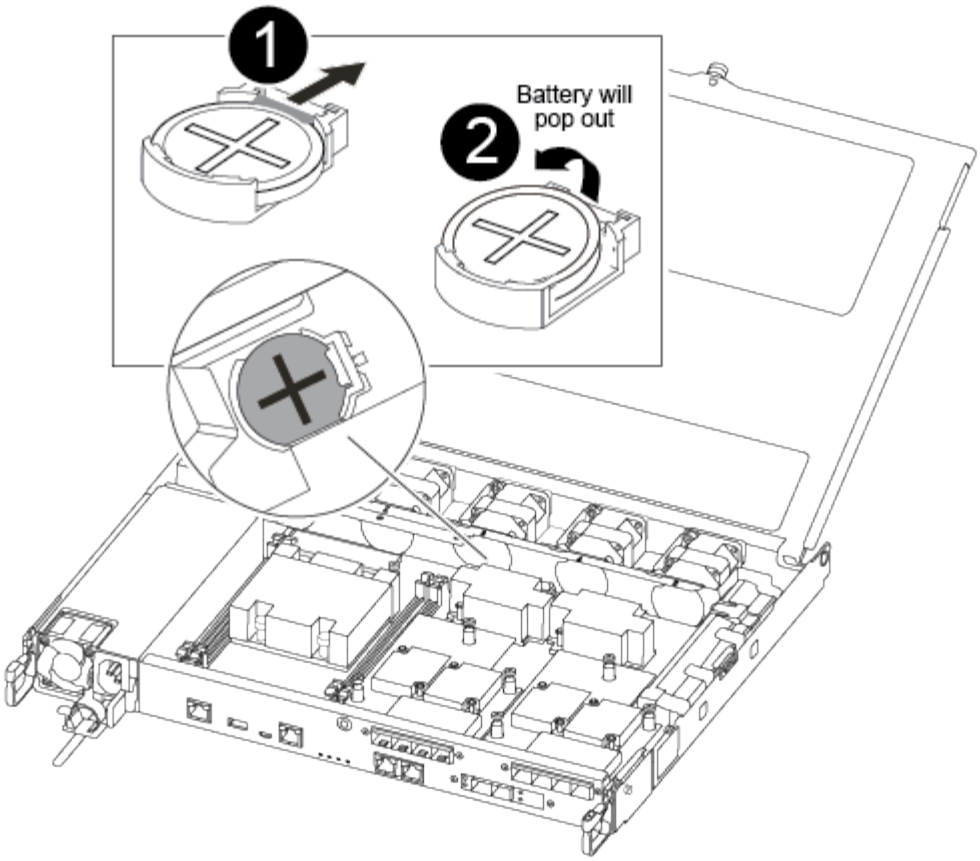
**Step 3: Replace the RTC battery**

To replace the RTC battery, locate it inside the controller and follow the specific sequence of steps.

You can use the following video or the tabulated steps to replace the RTC battery:

Replacing the RTC battery

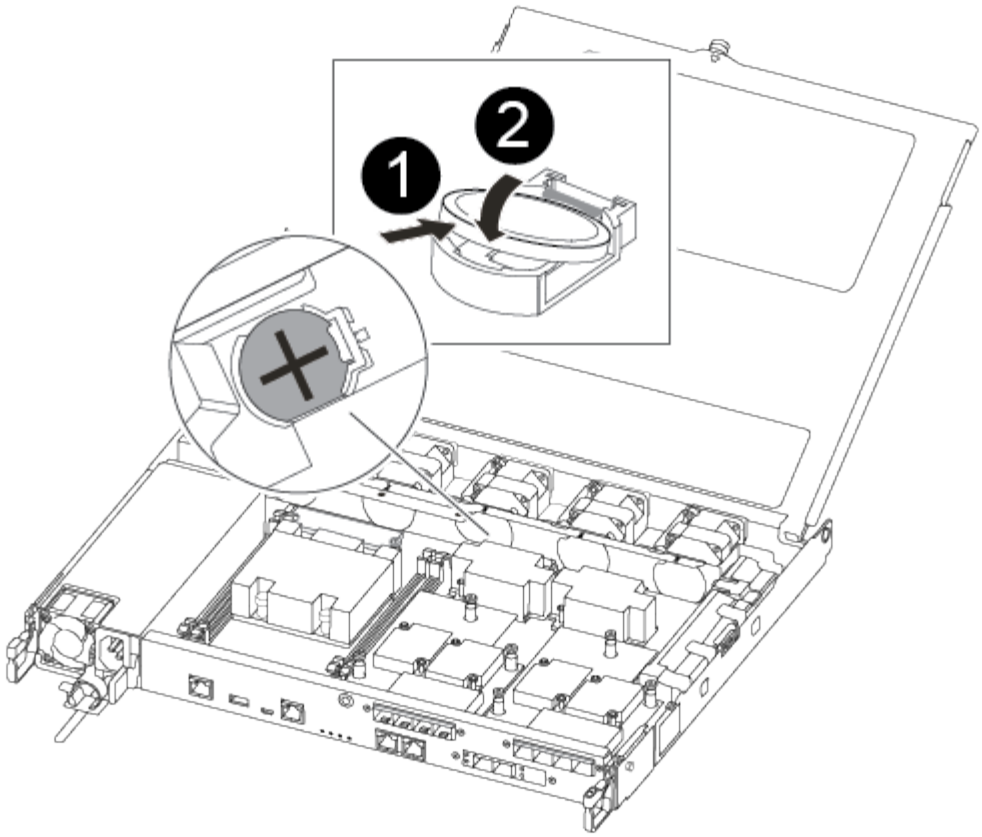
1. Locate the RTC battery between the heatsink and the midplane and remove it exactly as shown in the graphic.




| | |
|---|---|
| 1 | Gently pull tab away from the battery housing.<br><br>NOTE: Pulling it away aggressively might displace the tab. |
| 2 | Lift the battery up.<br><br>Make a note of the polarity of the battery. |
| 3 | The battery should eject out. |

The battery will be ejected out.

2. Remove the replacement battery from the antistatic shipping bag.
3. Locate the RTC battery holder between the heatsink and the midplane and insert it exactly as shown in the graphic.



| | |
|---|---|
| 1 | With positive polarity face up, slide the battery under the tab of the battery housing. |
| 2 | Push the battery gently into place and make sure the tab secures it to the housing.<br><br>+<br>**CAUTION:**<br><br>+<br>Pushing it in aggressively might cause the battery to eject out again. |

4. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.

#### Step 4: Reinstall the controller module and set time/date after RTC battery replacement

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. Insert the controller module into the chassis:

   a. Ensure the latching mechanism arms are locked in the fully extended position.
   b. Using both hands, align and gently slide the controller module into the latching mechanism arms until it stops.
   c. Place your index fingers through the finger holes from the inside of the latching mechanism.
   d. Press your thumbs down on the orange tabs on top of the latching mechanism and gently push the controller module over the stop.
   e. Release your thumbs from the top of the latching mechanisms and continue pushing until the latching mechanisms snap into place.

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

   f. Halt the controller at the LOADER prompt.

   The controller module should be fully inserted and flush with the edges of the chassis.

6. Reset the time and date on the controller:

   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, 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 controller.

7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller 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: Complete the replacement process

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

# FAS2600 System Documentation

## Install and setup

### Cluster configuration worksheet - FAS2600

You can use the worksheet to gather and record your site-specific IP addresses and other information required when configuring an ONTAP cluster.

Cluster Configuration Worksheet

### Start here: Choose your installation and setup experience

You can choose from different content formats to guide you through installing and setting up your new storage system.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

### Installation and setup PDF poster - FAS2600

You can use the PDF poster to install and set up your new system. The AFF FAS2600 Installation and Setup Instructions provides step-by-step instructions with live links to additional content.

### Installation and setup video - FAS2600

The following video shows end-to-end software configuration for systems running ONTAP 9.2.

AFF FAS2600 Setup Video

## Maintain

### Boot media

#### Overview of boot media replacement - FAS2600

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` file.

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 must be connected to a network to restore the `var` file system.
- For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.

- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

#### Check onboard encryption keys - FAS2600

## Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check what version of ONTAP the system is running.

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

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 the NetApp Encryption overview with the CLI.

**Steps**

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. 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`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to [Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier].
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to [Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later].
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy

controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

### Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

#### Steps

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

### Verify NVE configuration

#### Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps.
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes` manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- Shut down the impaired controller.

b. If the `Restored` column displays anything other than `yes`:

- Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

- Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
- Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
- Enter the command to display the OKM backup information: `security key-manager backup show`
- Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shutdown the controller.

### Verify NSE configuration

#### Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:

   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

   If the command fails, contact NetApp Support.

   mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers

display `available`: `security key-manager query`

c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to back up the OKM information: `security key-manager backup show`

        > Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

      - Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shut down the controller.

**Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later**

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`

   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.

- If no disks are shown, NSE is not configured.
- If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

### Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. Shut down the impaired controller.

  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

     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.

     mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

     c. Shut down the impaired controller.

  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

     a. Enter the onboard security key-manager sync command: `security key-manager onboard`

`sync`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

### Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

     b. Enter the command to display the key management information: `security key-manager onboard show-backup`

     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

     d. Return to admin mode: `set -priv admin`

     e. You can safely shut down the controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   g. Return to admin mode: `set -priv admin`
   h. You can safely shut down the controller.

#### Shut down the impaired controller - FAS2600

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. |

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

1. 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.

#### Replace the boot media - FAS2600

## 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.

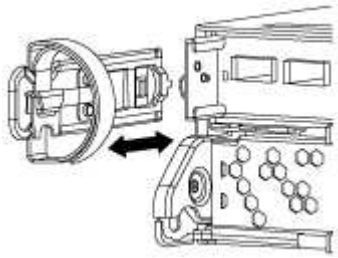
### Step 1: Remove the controller module

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.

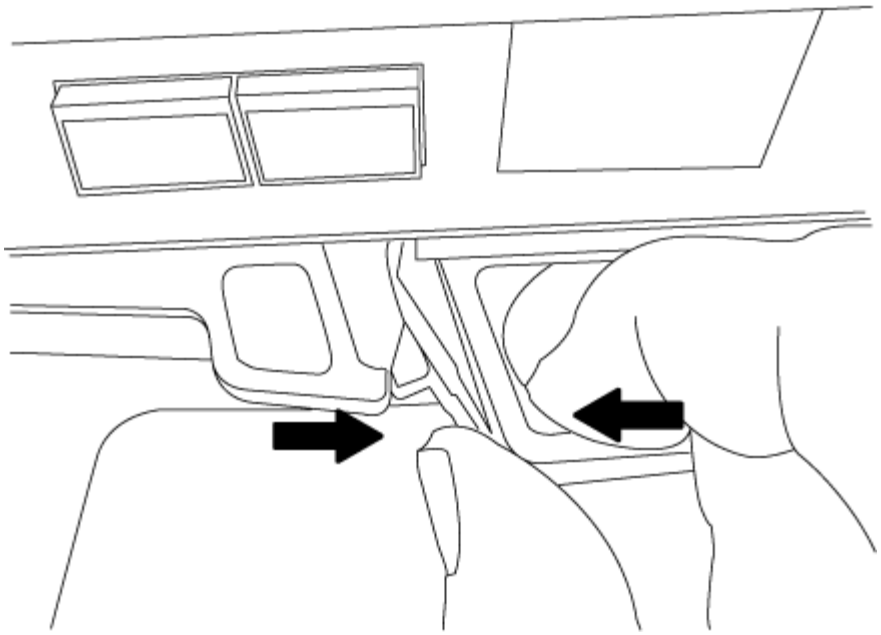
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

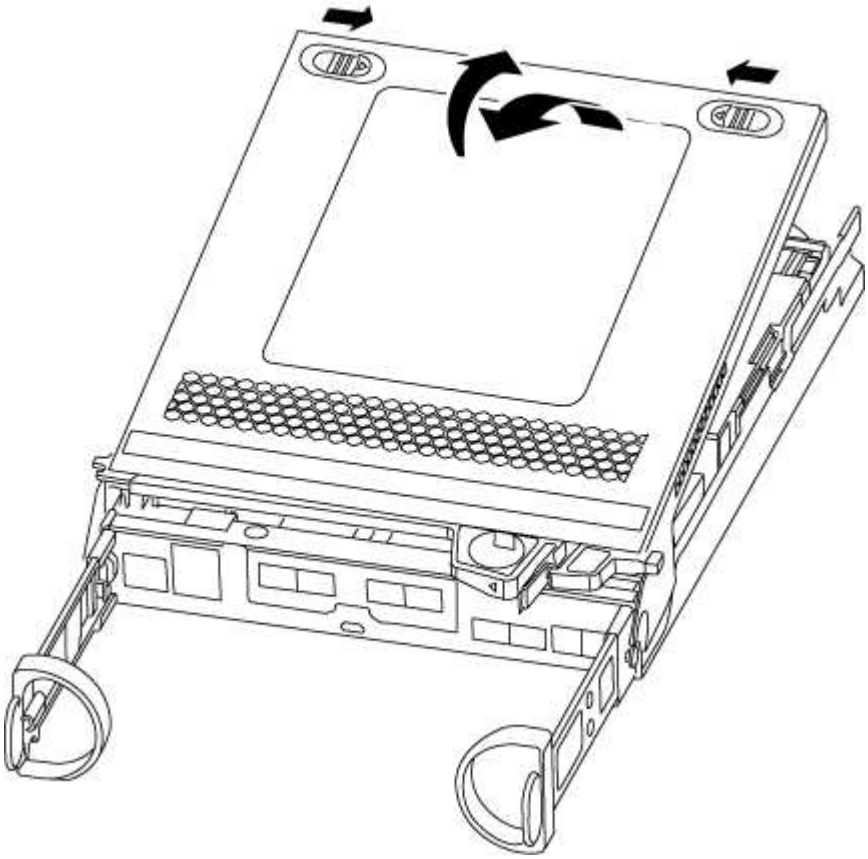
3. Remove and set aside the cable management devices from the left and right sides of the controller module.



4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.

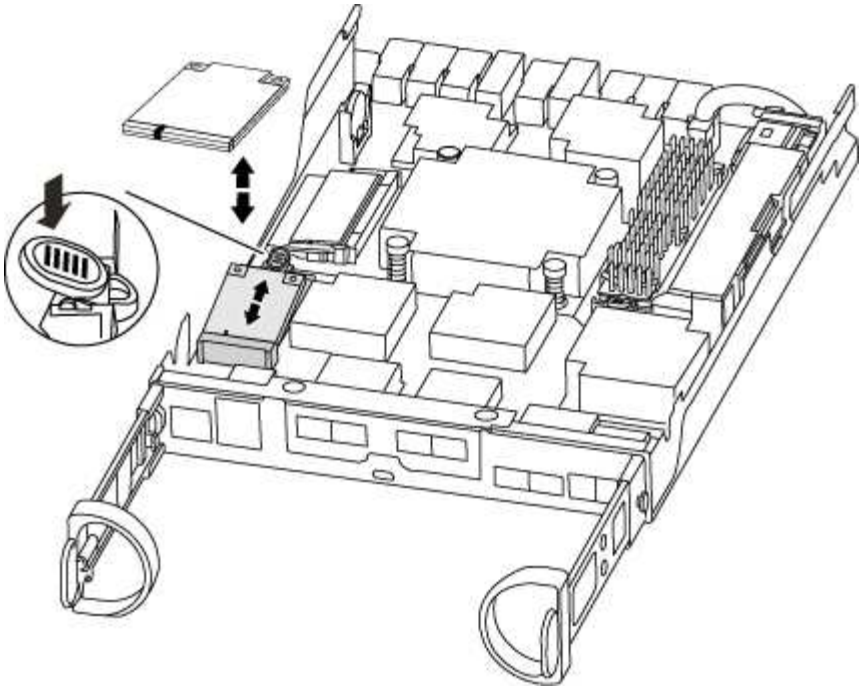


5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.



**Step 2: Replace the boot media**

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



3. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

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

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

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

6. Push the boot media down to engage the locking button on the boot media housing.
7. Close the controller module cover.

### 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 an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

**Steps**

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs) if they were removed.

3. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, push the cam handle to the closed position, and then tighten the thumbscrew.

   The controller 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 controller to boot to LOADER.

6. For systems with one controller in the chassis, reconnect the power and turn on the power supplies.

   The system begins to boot and stops at the LOADER prompt.

7. 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 controller from the healthy controller 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.

#### Boot the recovery image - FAS2600

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

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

4. Ensure that the environmental variables are set as expected:
   a. Take the controller 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 `setenvenvironment_variable_name changed_value` command.
   d. Save your changes using the `saveenv` 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 controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

7. Connect the console cable to the partner controller.
8. Give back the controller 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 controller 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.

#### Restore OKM, NSE, and NVE as needed - FAS2600

## Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

### Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

#### Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
| --- | --- |
| The LOADER prompt | Boot the controller to the boot menu: `boot_ontap menu` |
| Waiting for giveback… | a. Enter `Ctrl-C` at the prompt<br>b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y`<br>c. At the LOADER prompt, enter the `boot_ontap menu` command. |

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

   > The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:

   
   ```
   ---------------------------BEGIN BACKUP---------------------------
   TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
   QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
   dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
   3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
   IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
   LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
   ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   .
   .
   .
   .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAA

   ---------------------------END BACKUP---------------------------
   ```
   

7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.

9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.
12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.
    b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
14. If you are running ONTAP 9.6 or later:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

### Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

**Steps**

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
|---|---|
| The login prompt | Go to Step 7. |
| Waiting for giveback… | a. Log into the partner controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

`revert` command.

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

      Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.

12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

### Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

#### Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
| --- | --- |
| The login prompt | Go to Step 7. |
| Waiting for giveback… | a. Log into the partner controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

  Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

#### Return the failed part to NetApp - FAS2600

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Replace the caching module - FAS2600

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation.

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

AFF FAS2600 caching module replacement video

#### 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.

**About this task**

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.

ONTAP 9 System Administration Reference

You might want to erase the contents of your caching module before replacing it.

1. Although data on the caching module is encrypted, you might want to erase any data from the impaired caching module and verify that the caching module has no data:
   a. Erase the data on the caching module: `system controller flash-cache secure-erase run`
   b. Verify that the data has been erased from the caching module: `system controller flash-cache secure-erase show -node node_name`

      The output should display the caching module status as erased.
2. If the impaired controller is part of an HA pair, 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 `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller:<br>• For an HA pair, take over the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.<br>• For a stand-alone system: `system node halt` *`impaired_node_name`* |

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

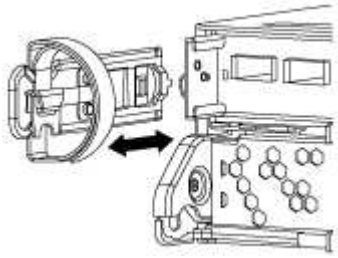
#### Step 2: Remove controller module

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.

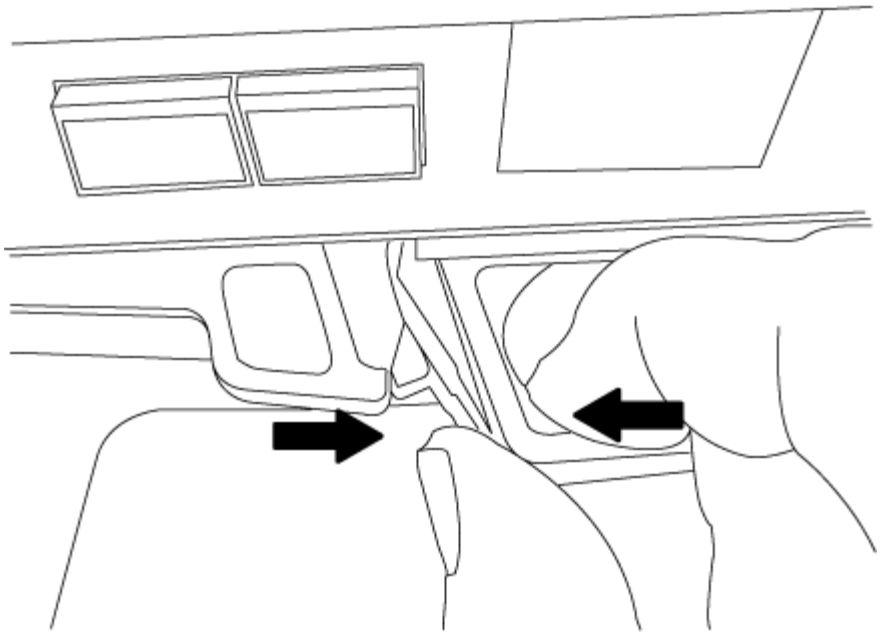
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

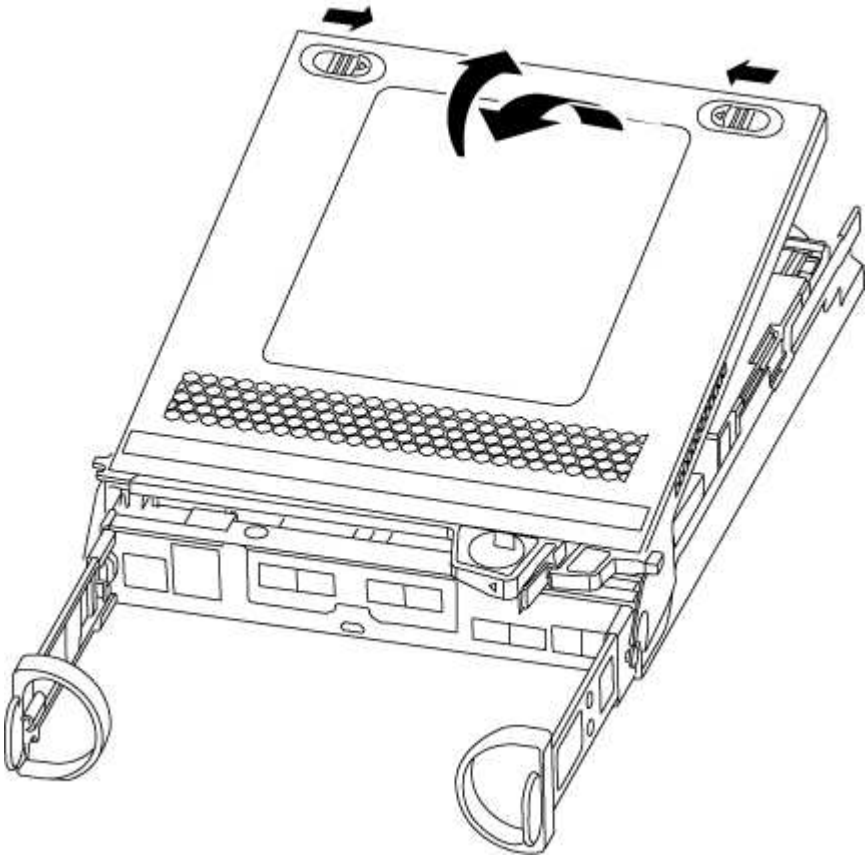
3. Remove and set aside the cable management devices from the left and right sides of the controller module.



4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.



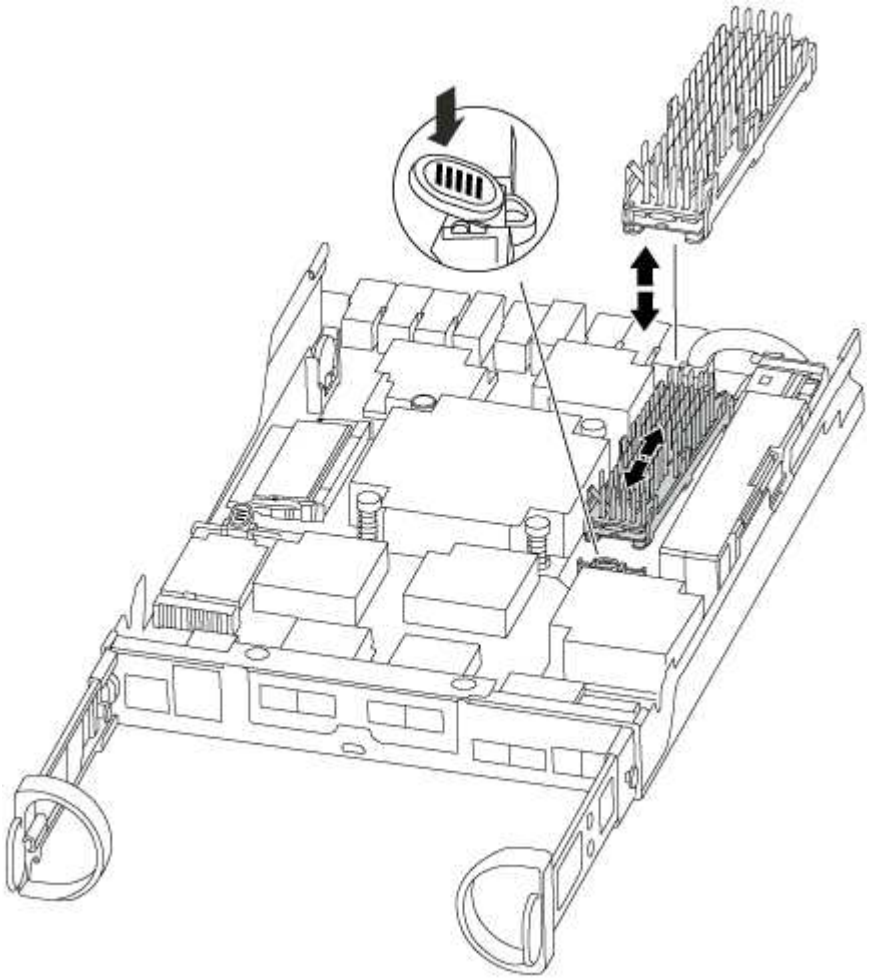
**Step 3: Replace a caching module**

To replace a caching module referred to as the M.2 PCIe card on the label on your controller, locate the slot inside the controller and follow the specific sequence of steps.

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

1. Locate the caching module at the rear of the controller module and remove it.
   a. Press the release tab.
   b. Remove the heatsink.



1. Gently pull the caching module straight out of the housing.
2. Align the edges of the caching module with the socket in the housing, and then gently push it into the socket.
3. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

4. Reseat and push the heatsink down to engage the locking button on the caching module housing.
5. Close the controller module cover, as needed.

#### Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

1. If you have not already done so, replace the cover on the controller module.
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. Complete the reinstallation of the controller module:

| If your system is in… | Then perform these steps… |
|---|---|
| An HA pair | The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.<br><br>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.<br><br>> Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br><br>The controller begins to boot as soon as it is seated in the chassis.<br><br>b. If you have not already done so, reinstall the cable management device.<br><br>c. Bind the cables to the cable management device with the hook and loop strap.<br><br>d. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process.<br><br>> If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br><br>e. Select the option to boot to Maintenance mode from the displayed menu. |

| If your system is in… | Then perform these steps… |
| --- | --- |
| A stand-alone configuration | 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.<br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. Bind the cables to the cable management device with the hook and loop strap.<br>d. Reconnect the power cables to the power supplies and to the power sources, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message.<br>If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br>e. From the boot menu, select the option for Maintenance mode. |

**Step 5: Run system-level diagnostics**

After installing a new caching module, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the caching module: `sldiag device run -dev fcache`
4. Verify that no hardware problems resulted from the replacement of the caching module: `sldiag device status -dev fcache -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

| If the system-level diagnostics tests… | Then… |
|---|---|
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br><br>The following default response is displayed:<br><br>SLDIAG: No log messages are present.<br><br>c. Exit Maintenance mode: `halt`<br><br>The controller displays the LOADER prompt.<br><br>d. Boot the controller from the LOADER prompt: `bye`<br>e. Return the controller to normal operation:<br><br>**If your controller is in an HA pair**, perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`*<br><br>**Note:** If you disabled automatic giveback, re-enable it with the `storage failover modify` command.<br><br>**If your controller is in a stand-alone configuration**, proceed to the next step. No action is required.<br><br>You have completed system-level diagnostics. |

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

#### 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 & Replacements page for further information.

### Chassis

#### Overview of chassis replacement - FAS2600

To replace the chassis, you must move the power supplies, 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.

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 written with the assumption that you are moving all drives and controller module or modules to the new chassis, and that the chassis is a new component from NetApp.
- 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.

AFF FAS2600 chassis replacement video

#### Shut down the controllers - FAS2600

## You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

### About this task

- If you have a cluster with more than two controllers, 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 the Administration overview with the CLI.
- 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`

### Steps

1. If your system has two controller modules, disable the HA pair.

| If your system is running clustered ONTAP with… | Then… |
|---|---|
| Two controllers in the cluster | `cluster ha modify -configured false` `storage failover modify -node node0 -enabled false` |
| More than two controllers in the cluster | `storage failover modify -node node0 -enabled false` |

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

> You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node *second_node_name* -ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

#### Move and replace hardware - FAS2600

## Move the power supplies, 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: Move the power supply

Moving out a power supply when replacing a chassis involves turning off, disconnecting, and removing the power supply from the old chassis and installing and connecting it on the replacement 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. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.
4. Use the cam handle to slide the power supply out of the system.

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

5. Repeat the preceding steps for any remaining power supplies.
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 using the cam handle.

   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. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
8. 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.

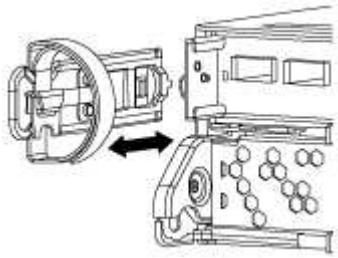
**Step 2: Remove the controller module**

Remove the controller module or modules from the old chassis.

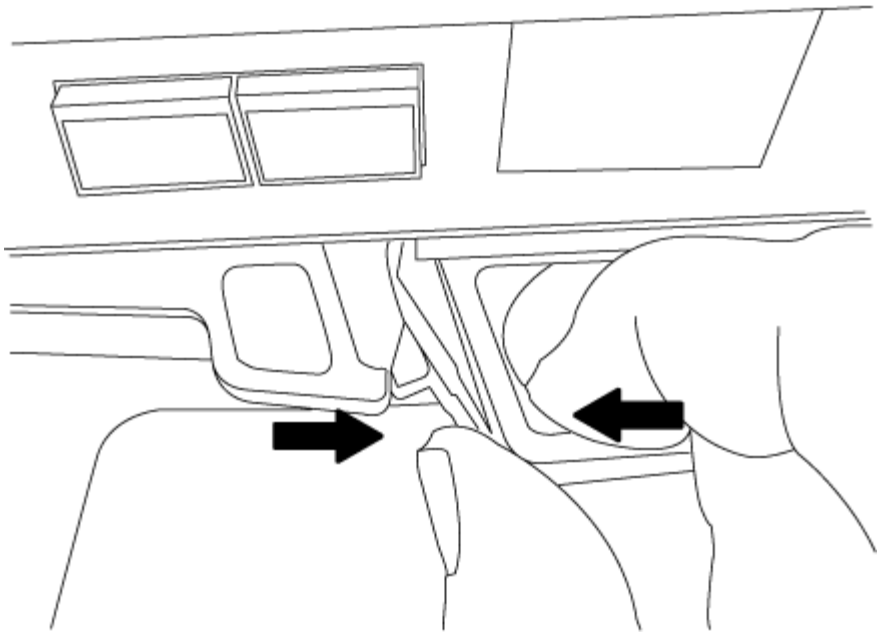
1. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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



3. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module 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 3: Move drives to the new chassis**

Move the drives from each bay opening in the old chassis to the same bay opening in the new chassis.

1. Gently remove the bezel from the front of the system.
2. Remove the drives:
   a. Press the release button at the top of the carrier face below the LEDs.
   b. Pull the cam handle to its fully open position to unseat the drive from the midplane, and then gently slide the drive out of the chassis.

      The drive should disengage from the chassis, allowing it to slide free of the chassis.

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

      Drives are fragile. Handle them as little as possible to prevent damage to them.
3. Align the drive from the old chassis with the same bay opening in the new chassis.
4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate upward.
5. Firmly push the drive the rest of the way into the chassis, and then lock the cam handle by pushing it up and against the drive holder.

   Be sure to close the cam handle slowly so that it aligns correctly with the front of the drive carrier. It clicks when it is secure.
6. Repeat the process for the remaining drives in the system.

### Step 4: Replace a chassis from within the equipment rack or system cabinet

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.
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. If you have not already done so, install the bezel.

### Step 5: Install the controller

After you install the controller module and any other components into the new chassis, boot it to a state where you can run the interconnect diagnostic test.

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.

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. Repeat the preceding steps if there is a second controller to install in the new chassis.
4. Complete the installation of the controller module:

| If your system is in… | Then perform these steps… |
| --- | --- |
| An HA pair | 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.<br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. Bind the cables to the cable management device with the hook and loop strap.<br>d. Repeat the preceding steps for the second controller module in the new chassis. |
| A stand-alone configuration | 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.<br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. Bind the cables to the cable management device with the hook and loop strap.<br>d. Reinstall the blanking panel and then go to the next step. |

5. Connect the power supplies to different power sources, and then turn them on.
6. Boot each controller to Maintenance mode:
   a. As each controller 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.

#### Restore and verify the configuration - FAS2600

You must verify the HA state of the chassis, run diagnostics, 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.

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`
      - `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. The next step depends on your system configuration.

| If your system is in… | Then… |
|---|---|
| A stand-alone configuration | a. Exit Maintenance mode: `halt`<br>b. Go to "Completing the replacement process. |
| An HA pair with a second controller module | Exit Maintenance mode: `halt`<br>The LOADER prompt appears. |

### Step 2: Run system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second controller if you are in an HA configuration.

> Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

| If the system-level diagnostics tests… | Then… |
|---|---|
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>`SLDIAG: No log messages are present.`<br>c. Exit Maintenance mode on both controllers: `halt`<br>The system displays the LOADER prompt.<br>You must exit Maintenance mode on both controllers before proceeding any further.<br>d. Enter the following command on both controllers at the LOADER prompt: `bye`<br>e. Return the controller to normal operation: |

| If your system is running ONTAP… | Then… |
| --- | --- |
| With two nodes in the cluster | Issue these commands: `node::> cluster ha modify -configured true node::> storage failover modify -node node0 -enabled true` |
| With more than two nodes in the cluster | Issue this command: `node::> storage failover modify -node node0 -enabled true` |
| In a stand-alone configuration | You have no further steps in this particular task.<br><br>You have completed system-level diagnostics. |
| Resulted in some test failures | Determine the cause of the problem.<br><br>a. Exit Maintenance mode: `halt`<br>b. Perform a clean shutdown, and then disconnect the power supplies.<br>c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Reconnect the power supplies, and then power on the storage system.<br>e. Rerun the system-level diagnostics test. |

#### 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 & Replacements page for further information.

### Controller module

#### Overview of controller module replacement - FAS2600

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 is in an HA pair, the healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- This procedure includes steps for automatically or manually reassigning drives to the *replacement* controller, depending on your system’s configuration.

  You should perform the drive reassignment as directed in the procedure.

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

provider.

- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller 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* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller'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 controller - FAS2600

## 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 the Administration overview with the CLI.

**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_down_h`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. If the impaired controller is part of an HA pair, 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 Remove controller module.. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y`. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>+<br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

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

#### Replace the controller module hardware - FAS2600

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

AFF FAS2600 controller replacement video

### Step 1: Remove controller module

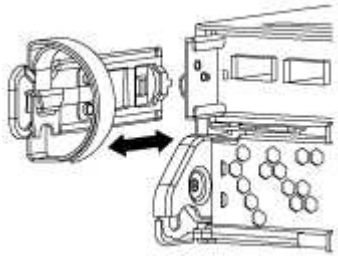
To replace the controller module, you must first remove the old controller module from the chassis.

#### Steps

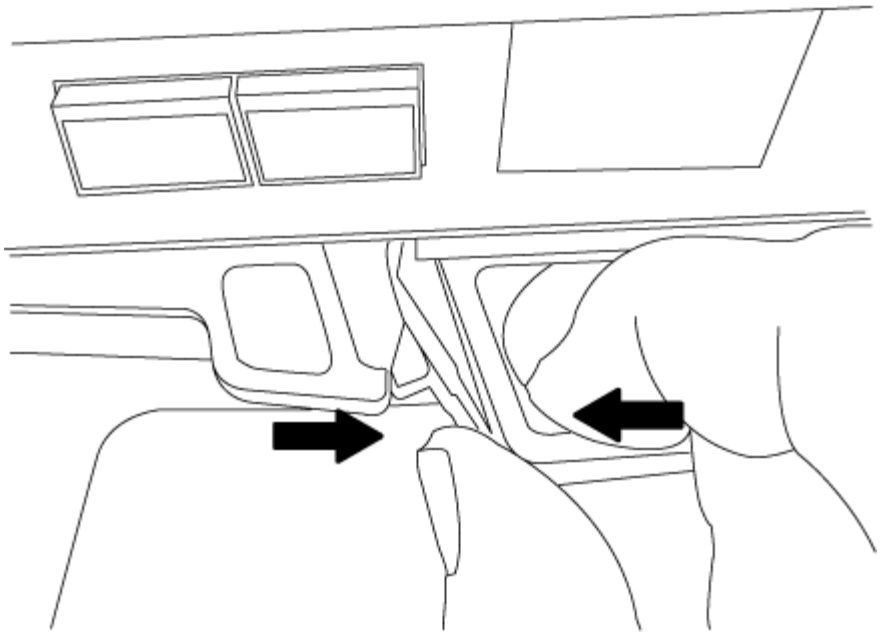
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

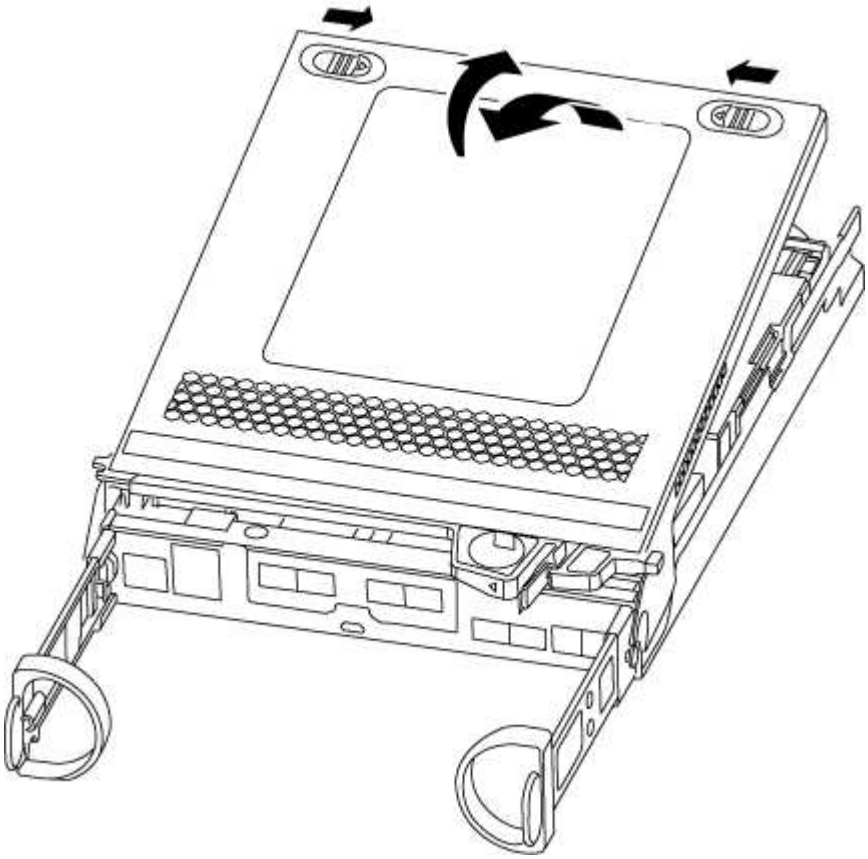
3. Remove and set aside the cable management devices from the left and right sides of the controller module.



4. If you left the SFP modules in the system after removing the cables, move them to the new controller module.
5. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



6. Turn the controller module over and place it on a flat, stable surface.
7. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

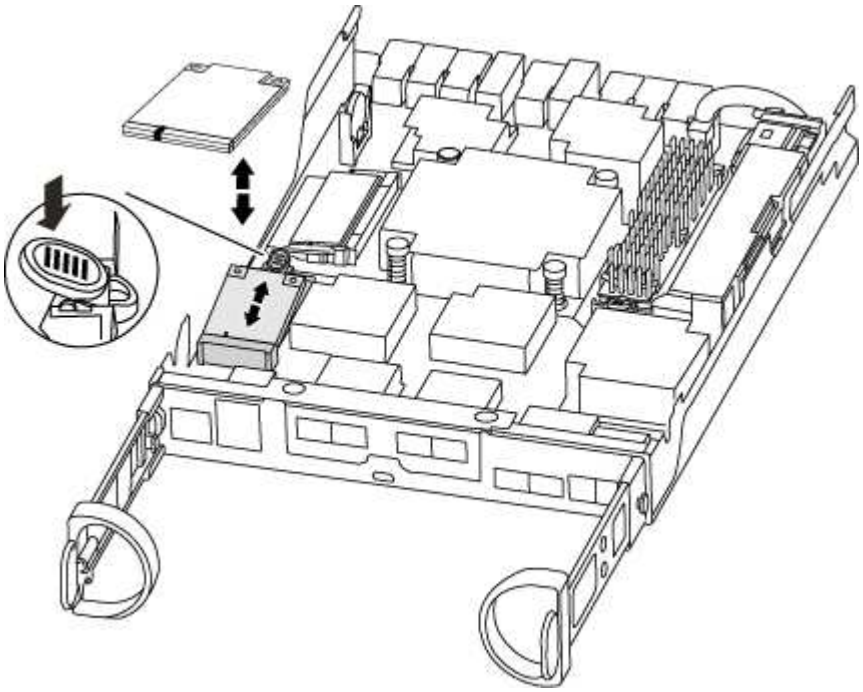


**Step 2: Move the boot media**

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

**Steps**

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



2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

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

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

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

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

### Step 3: Move the NVMEM battery

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

**Steps**

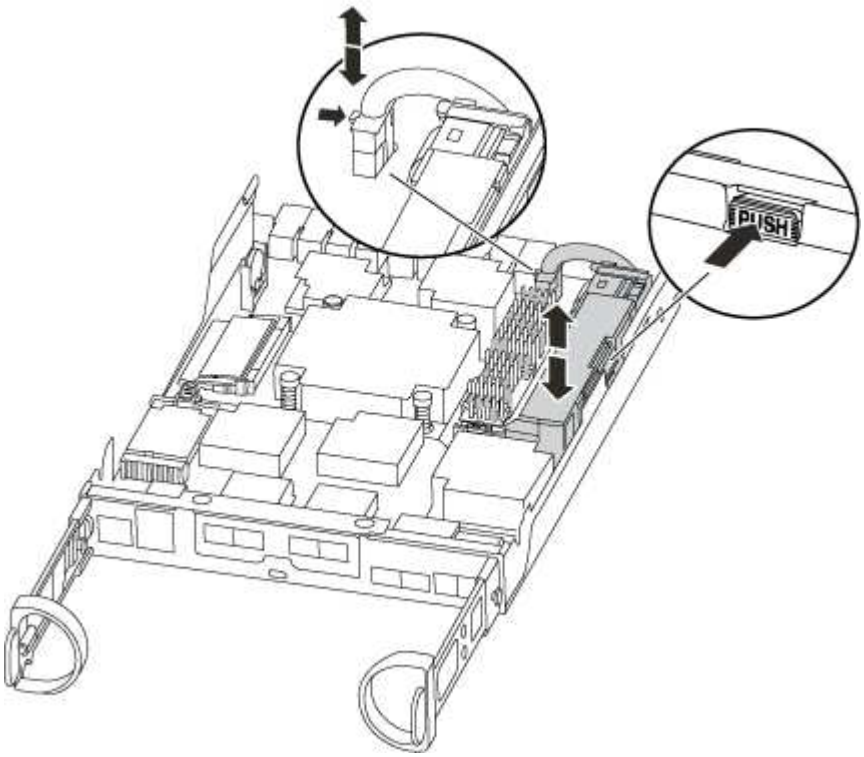
1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

- If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
- If the LED is on and power is on, unwritten data is stored on NVMEM.

  This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Locate the NVMEM battery in the controller module.




3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
5. Move the battery to the replacement controller module.
6. Loop the battery cable around the cable channel on the side of the battery holder.
7. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
8. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.

### Step 4: Move the DIMMs

To move the DIMMs, you must follow the directions to locate and move them from the old controller module into the replacement controller module.

You must have the new controller module ready so that you can move the DIMMs directly from the impaired controller module to the corresponding slots in the replacement controller module.

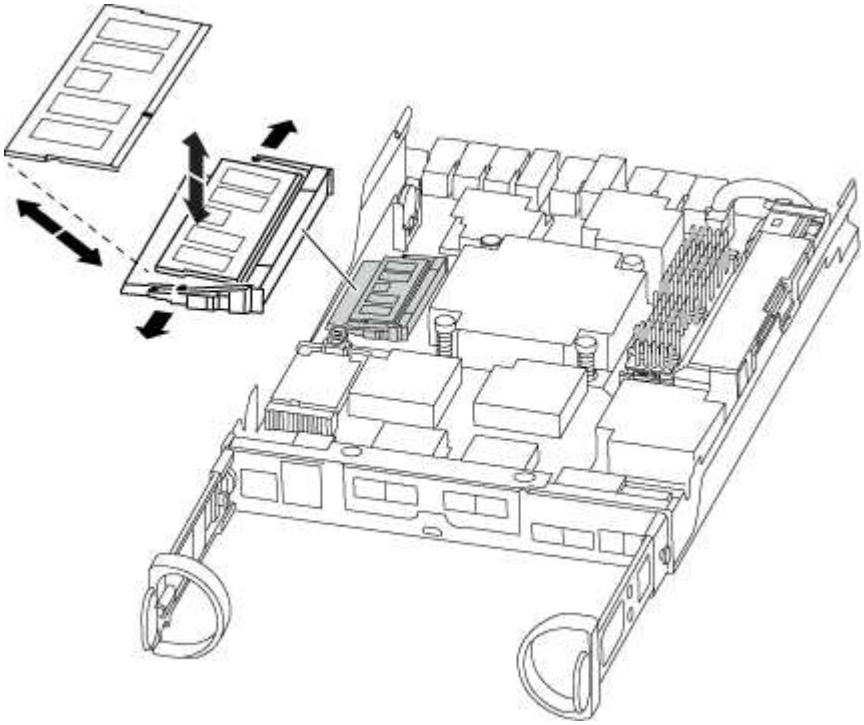
**Steps**

1. Locate the DIMMs on your controller module.
2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

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

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

   The following illustration shows the location of system DIMMs:



4. Repeat these steps to remove additional DIMMs as needed.
5. Verify that the NVMEM battery is not plugged into the new controller module.
6. Locate the slot where you are installing the DIMM.
7. 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.

8. Repeat these steps for the remaining DIMMs.
9. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

   Make sure that the plug locks down onto the controller module.

### Step 5: Move the caching module

To move a caching module referred to as the M.2 PCIe card on the label on your controller, locate and move it from the old controller into the replacement controller and follow the specific sequence of steps.

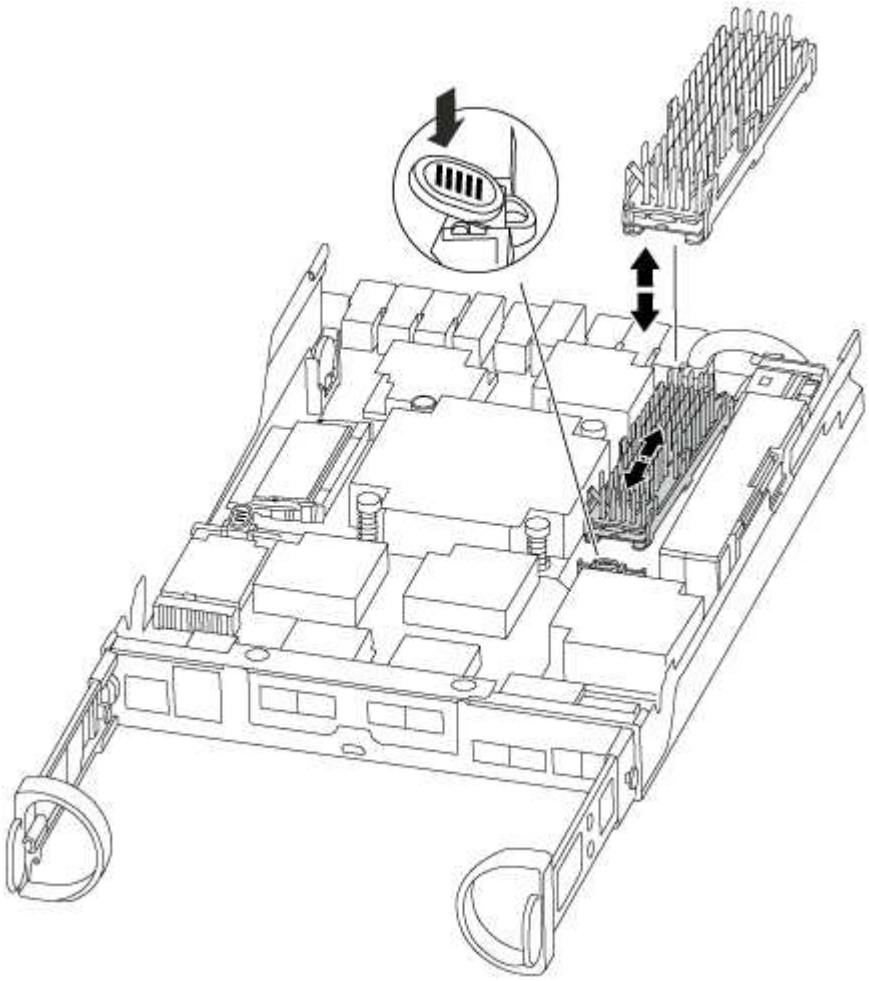
You must have the new controller module ready so that you can move the caching module directly from the old controller module to the corresponding slot in the new one. All other components in the storage system must be functioning properly; if not, you must contact technical support.

#### Steps

1. Locate the caching module at the rear of the controller module and remove it.

   a. Press the release tab.

   b. Remove the heatsink.



2. Gently pull the caching module straight out of the housing.
3. Move the caching module to the new controller module, and then align the edges of the caching module with the socket housing and gently push it into the socket.
4. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

5. Reseat and push the heatsink down to engage the locking button on the caching module housing.
6. Close the controller module cover, as needed.

### Step 6: Install the controller

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

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:

| If your system is in… | Then perform these steps… |
| --- | --- |
| An HA pair | The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.<br><br>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.<br><br>ⓘ Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br><br>The controller begins to boot as soon as it is seated in the chassis.<br><br>b. If you have not already done so, reinstall the cable management device.<br><br>c. Bind the cables to the cable management device with the hook and loop strap.<br><br>d. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process.<br><br>ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br><br>e. Select the option to boot to Maintenance mode from the displayed menu. |

| If your system is in… | Then perform these steps… |
| --- | --- |
| A stand-alone configuration | 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.<br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. Bind the cables to the cable management device with the hook and loop strap.<br>d. Reconnect the power cables to the power supplies and to the power sources, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message.<br>If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br>e. From the boot menu, select the option for Maintenance mode. |

**Important:** During the boot process, you might see the following prompts:

- A prompt warning of a system ID mismatch and asking to override the system ID.
- A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
  You can safely respond `y` to these prompts.

#### Restore and verify the system configuration - FAS2600

## 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 after replacing the controller

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

#### About this task

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

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

**Steps**

1. 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: `show date`

   The date and time are given in GMT.

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 HA state of the controller module

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

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

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

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

   - `ha`
   - `non-ha`

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

### Step 3: Run system-level diagnostics

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

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

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `halt`

After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

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

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

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

4. Run diagnostics as desired.

| If you want to run diagnostic tests on… | Then… |
| --- | --- |
| Individual components | a. Clear the status logs: `sldiag device clearstatus`<br>b. Display the available tests for the selected devices: `sldiag device show -dev` *`dev_name`*<br><br>*dev_name* can be any one of the ports and devices identified in the preceding step.<br><br>c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev` *`dev_name`* `-selection only`<br><br>-selection only disables all other tests that you do not want to run for the device.<br><br>d. Run the selected tests: `sldiag device run -dev` *`dev_name`*<br><br>After the test is complete, the following message is displayed:<br><br>`*> <SLDIAG:_ALL_TESTS_COMPLETED>`<br><br>e. Verify that no tests failed: `sldiag device status -dev` *`dev_name`* `-long -state failed`<br><br>System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component. |

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

5. Proceed based on the result of the preceding step.

| If the system-level diagnostics tests… | Then… |
| --- | --- |
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>`SLDIAG: No log messages are present.`<br>c. Exit Maintenance mode: `halt`<br>The system displays the LOADER prompt.<br>You have completed system-level diagnostics. |
| Resulted in some test failures | Determine the cause of the problem.<br>a. Exit Maintenance mode: `halt`<br>b. Perform a clean shutdown, and then disconnect the power supplies.<br>c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Reconnect the power supplies, and then power on the storage system.<br>e. Rerun the system-level diagnostics test. |

#### Recable the system and reassign disks - FAS2600

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

### Step 1: Recable the system

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

**Steps**

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.

d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

### Step 2: Reassign disks

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

#### Option 1: Verify the system ID change on an HA system

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

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

1. If the *replacement* controller 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* controller, boot the controller, 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* controller console and then, from the healthy controller, 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 controller, 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`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, 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 controller:

a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode replacement_node_name`

The *replacement* controller 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 content 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* controller 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 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

7. Verify that the expected volumes are present for each controller: `vol show -node node-name`

8. If you disabled automatic takeover on reboot, enable it from the healthy controller: `storage failover modify -node replacement-node-name -onreboot true`

### Option 2: Manually reassign the system ID on a stand-alone system in ONTAP

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

**About this task**

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

**Steps**

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by pressing Ctrl-C, and then select the option to boot to Maintenance mode from the displayed menu.
2. You must enter `Y` when prompted to override the system ID due to a system ID mismatch.
3. View the system IDs: `disk show -a`
4. You should make a note of the old system ID, which is displayed as part of the disk owner column.

   The following example shows the old system ID of 118073209:

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

     DISK      OWNER                   POOL   SERIAL NUMBER  HOME
   --------    -------------           -----  -------------  -------------
   disk_name    system-1  (118073209)  Pool0  J8XJE9LC       system-1
   (118073209)
   disk_name    system-1  (118073209)  Pool0  J8Y478RC       system-1
   (118073209)
   .
   .
   .
   ```

5. Reassign disk ownership by using the system ID information obtained from the disk show command: `disk reassign -s old system ID disk reassign -s 118073209`
6. Verify that the disks were assigned correctly: `disk show -a`

   The disks belonging to the replacement node should show the new system ID. The following example now show the disks owned by system-1 the new system ID, 118065481:

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

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

7. Boot the node: `boot_ontap`

#### Complete system restoration - FAS2600

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

### Step 1: Install licenses for the replacement controller in ONTAP

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

#### About this task

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

#### Before you begin

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.

#### 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: Restore Storage and Volume Encryption functionality

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

**Step**

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use 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

#### Step 3: Verify LIFs and register the serial number

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

**Steps**

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

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

2. Register the system serial number with NetApp Support.
   - 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. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

#### 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 & Replacements page for further information.

### Replace a DIMM - FAS2600

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

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.

AFF FAS2600 DIMM replacement video

#### Step 1: Shut down the impaired controller

Shut down or take over the impaired controller using different procedures, depending on the storage system hardware 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 the Administration overview with the CLI.

**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_down_h`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. If the impaired controller is part of an HA pair, 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 Remove controller module.. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y`. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br>+<br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

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

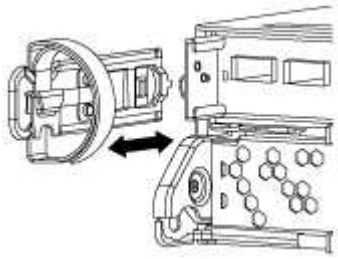
#### Step 2: Remove controller module

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.

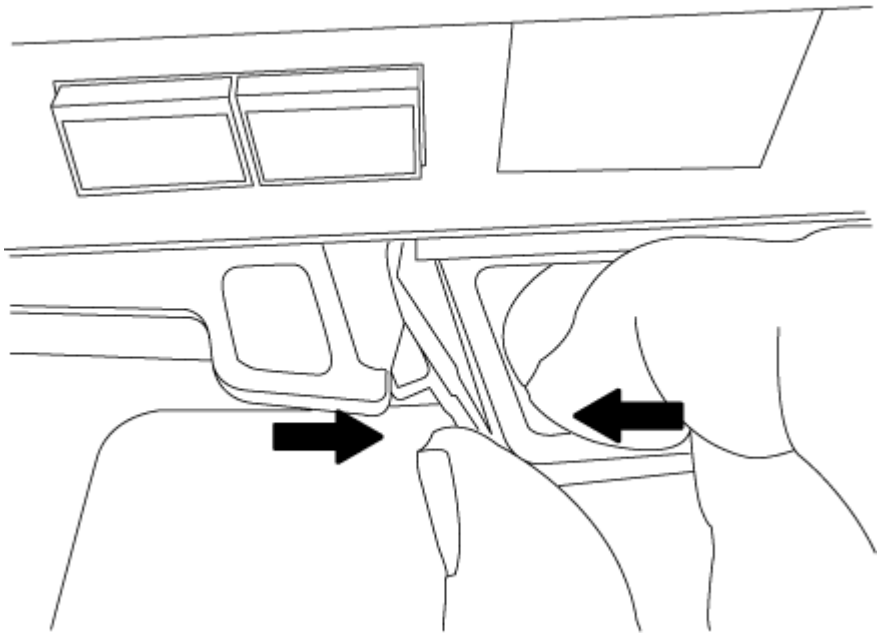
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

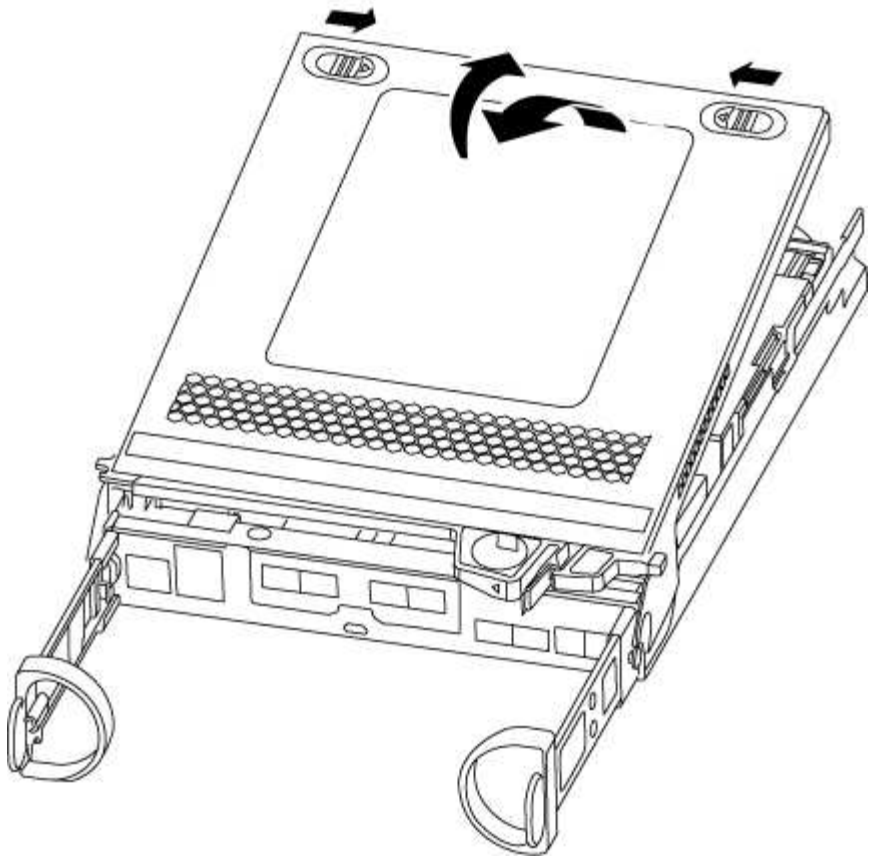
3. Remove and set aside the cable management devices from the left and right sides of the controller module.



4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.



**Step 3: Replace the DIMMs**

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

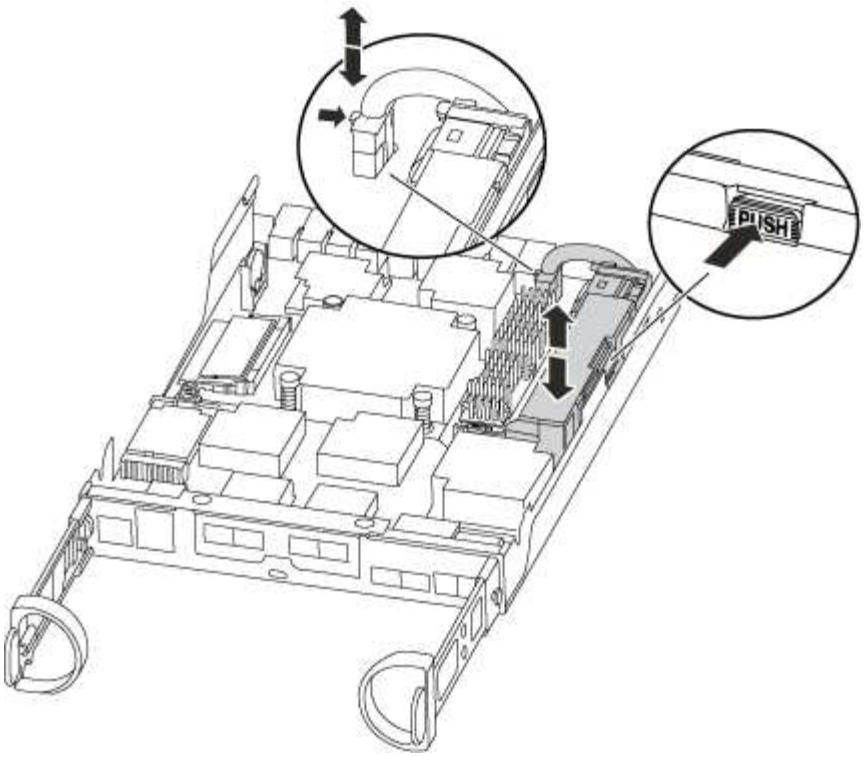
If you are replacing a DIMM, you need to remove it after you have unplugged the NVMEM battery from the controller module.

1. Check the NVMEM LED on the controller module.

   You must perform a clean system shutdown before replacing system components to avoid losing unwritten data in the nonvolatile memory (NVMEM). The LED is located on the back of the controller module. Look for the following icon:

2. If the NVMEM LED is not flashing, there is no content in the NVMEM; you can skip the following steps and proceed to the next task in this procedure.
3. If the NVMEM LED is flashing, there is data in the NVMEM and you must disconnect the battery to clear the memory:
   a. Locate the battery, press the clip on the face of the battery plug to release the lock clip from the plug socket, and then unplug the battery cable from the socket.




b. Confirm that the NVMEM LED is no longer lit.

c. Reconnect the battery connector.

4. Recheck the NVMEM LED.
5. Locate the DIMMs on your controller module.

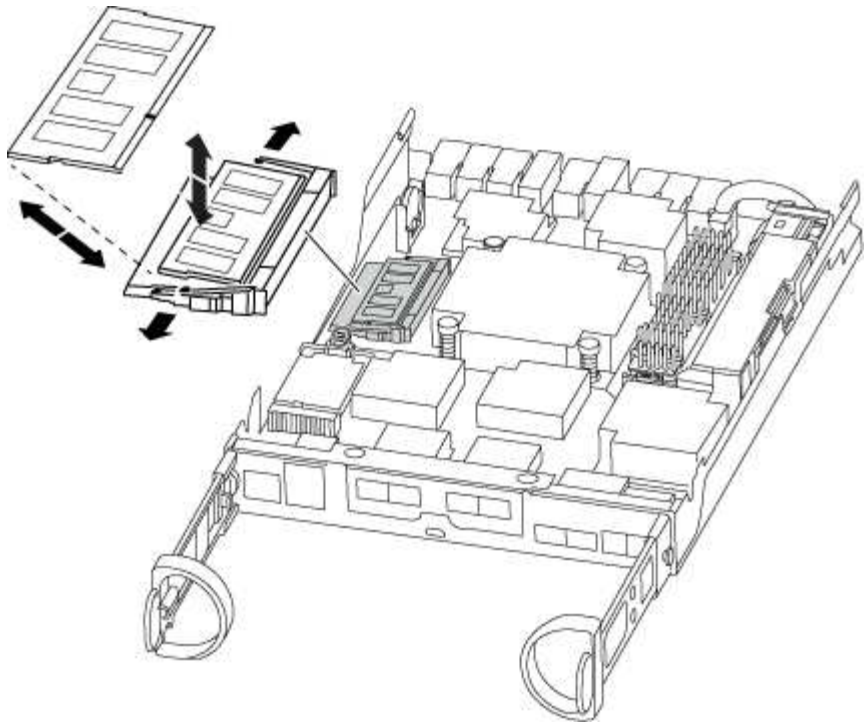
> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.

6. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
7. 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.

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

The following illustration shows the location of system DIMMs:



8. 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.

9. 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.

10. 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.
11. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

    Make sure that the plug locks down onto the controller module.

12. Close the controller module cover.

#### Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

1. If you have not already done so, replace the cover on the controller module.
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. Complete the reinstallation of the controller module:

| If your system is in… | Then perform these steps… |
| --- | --- |
| An HA pair | The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.<br><br>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.<br><br>ⓘ Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br><br>The controller begins to boot as soon as it is seated in the chassis.<br><br>b. If you have not already done so, reinstall the cable management device.<br><br>c. Bind the cables to the cable management device with the hook and loop strap.<br><br>d. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process.<br><br>ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br><br>e. Select the option to boot to Maintenance mode from the displayed menu. |

| If your system is in… | Then perform these steps… |
| --- | --- |
| A stand-alone configuration | 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.<br><br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br><br>b. If you have not already done so, reinstall the cable management device.<br><br>c. Bind the cables to the cable management device with the hook and loop strap.<br><br>d. Reconnect the power cables to the power supplies and to the power sources, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message.<br><br>If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br><br>e. From the boot menu, select the option for Maintenance mode. |

#### Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

| **If the system-level diagnostics tests…** | **Then…** |
|---|---|
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>SLDIAG: No log messages are present.<br>c. Exit Maintenance mode: `halt`<br>The controller displays the LOADER prompt.<br>d. Boot the controller from the LOADER prompt: `bye`<br>e. Return the controller to normal operation: |

| **If your controller is in…** | **Then…** |
|---|---|
| An HA pair | Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`*<br>If you disabled automatic giveback, re-enable it with the storage failover modify command. |
| A stand-alone configuration | Proceed to the next step.<br>No action is required.<br>You have completed system-level diagnostics. |

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

#### 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 & Replacements page for further information.

### Replace SSD Drive or HDD Drive - FAS2600

You can replace a failed drive nondisruptively while I/O is in progress. The procedure for replacing an SSD is meant for non-spinning drives and the procedure for replacing an HDD is meant for spinning drives.

When a drive fails, the platform logs a warning message to the system console indicating which drive has

failed. In addition, both the fault LED on the operator display panel and the fault LED on the failed drive are illuminated.

**Before you begin**

- Follow best practice and install the current version of the Disk Qualification Package (DQP) before replacing a drive.
- Identify the failed disk drive by running the `storage disk show -broken` command from the system console.

  The failed drive appears in the list of failed drives. If it does not, you should wait, and then run the command again.

  > Depending on the drive type and capacity, it can take up to several hours for the drive to appear in the list of failed drives.

- Determine whether SED authentication is enabled.

  How you replace the disk depends on how the disk drive is being used. If SED authentication is enabled, you must use the SED replacement instructions in the ONTAP 9 NetApp Encryption Power Guide. These Instructions describe additional steps you must perform before and after replacing an SED.

- Make sure the replacement drive is supported by your platform. See the NetApp Hardware Universe.
- Make sure all other components in the system are functioning properly; if not, you must contact technical support.

**About this task**

Drive firmware is automatically updated (nondisruptively) on new drives that have non current firmware versions.

When replacing several disk drives, you must wait one minute between the removal of each failed disk drive and the insertion of the replacement disk drive to allow the storage system to recognize the existence of each new disk.

**Procedure**

Replace the failed drive by selecting the option appropriate to the drives that your platform supports.

You may also choose to watch the Replace failed drive video that shows an overview of the embedded drive replacement procedure.

**Option 1: Replace SSD**

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Physically identify the failed drive.

   When a drive fails, the system logs a warning message to the system console indicating which drive failed. Additionally, the attention (amber) LED on the drive shelf operator display panel and the failed drive illuminate.

   > The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.

4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.

6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

7. Verify that the drive’s activity (green) LED is illuminated.

   When the drive’s activity LED is solid, it means that the drive has power. When the drive’s activity LED

is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

8. If you are replacing another drive, repeat Steps 3 through 7.
9. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
   a. Display all unowned drives: `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

      You can enter the command on either controller module.

      You can use the wildcard character to assign more than one drive at once.

   c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.

10. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

**Option 2: Replace HDD**

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the failed disk drive from the system console warning message and the illuminated fault LED on the disk drive
5. Press the release button on the disk drive face.

Depending on the storage system, the disk drives have the release button located at the top or on the left of the disk drive face.

For example, the following illustration shows a disk drive with the release button located on the top of the disk drive face:

The cam handle on the disk drive springs open partially and the disk drive releases from the midplane.

6. Pull the cam handle to its fully open position to unseat the disk drive from the midplane.

7. Slide out the disk drive slightly and allow the disk to safely spin down, which can take less than one minute, and then, using both hands, remove the disk drive from the disk shelf.
8. With the cam handle in the open position, insert the replacement disk drive into the drive bay, firmly pushing until the disk drive stops.

   Wait a minimum of 10 seconds before inserting a new disk drive. This allows the system to recognize that a disk drive was removed.

   If your platform drive bays are not fully loaded with drives, it is important to place the replacement drive into the same drive bay from which you removed the failed drive.

   Use two hands when inserting the disk drive, but do not place hands on the disk drive boards that are exposed on the underside of the disk carrier.

9. Close the cam handle so that the disk drive is fully seated into the midplane and the handle clicks into place.

   Be sure to close the cam handle slowly so that it aligns correctly with the face of the disk drive..

10. If you are replacing another disk drive, repeat Steps 4 through 9.
11. Reinstall the bezel.
12. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
    a. Display all unowned drives: `storage disk show -container-type unassigned`

       You can enter the command on either controller module.

    b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

       You can enter the command on either controller module.

       You can use the wildcard character to assign more than one drive at once.

    c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

       You must reenable automatic drive assignment on both controller modules.

13. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

### Replace the NVMEM battery - FAS2600

To replace an NVMEM battery in the system, you must remove the controller module from the system, open it, replace the battery, and close and replace the controller module.

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

AFF FAS2600 NVMEM battery replacement video

#### 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.

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 the Administration overview with the CLI.

**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_down_h`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. If the impaired controller is part of an HA pair, 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 Remove controller module.. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y`. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>+<br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

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

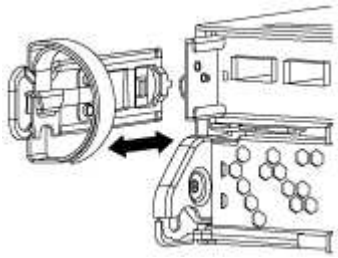
#### Step 2: Remove controller module

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.

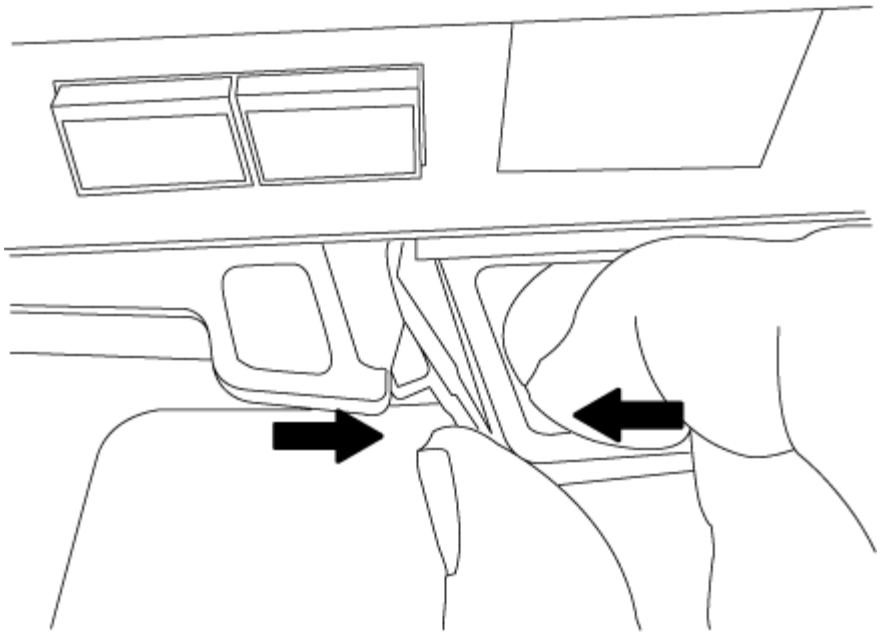
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

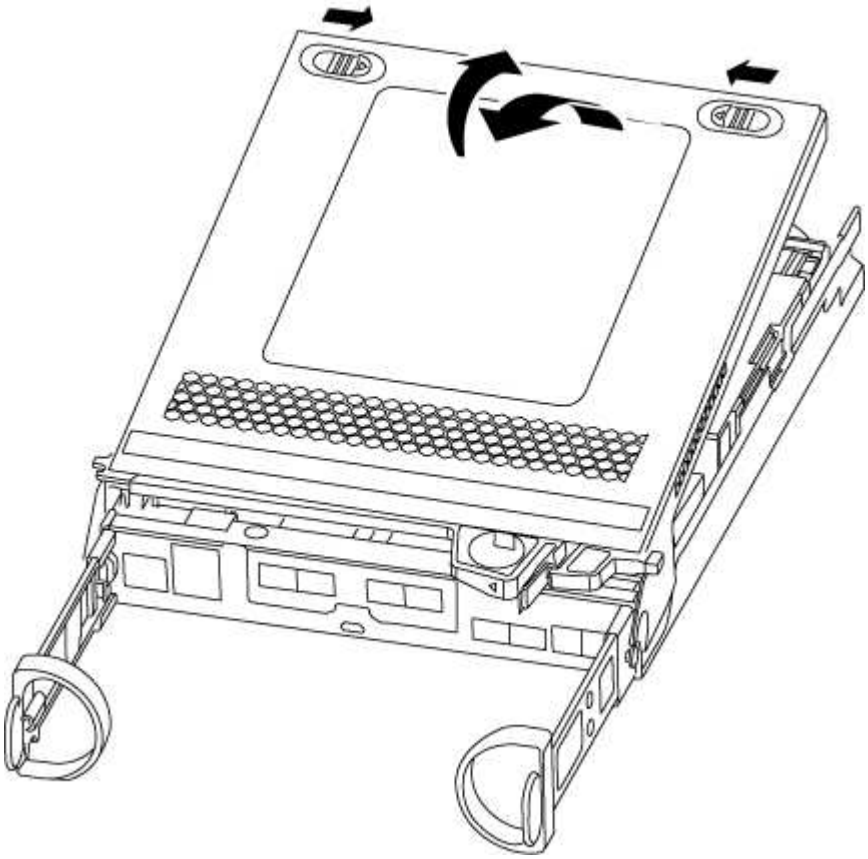
3. Remove and set aside the cable management devices from the left and right sides of the controller module.



4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.



**Step 3: Replace the NVMEM battery**

To replace the NVMEM battery in your system, you must remove the failed NVMEM battery from the system and replace it with a new NVMEM battery.

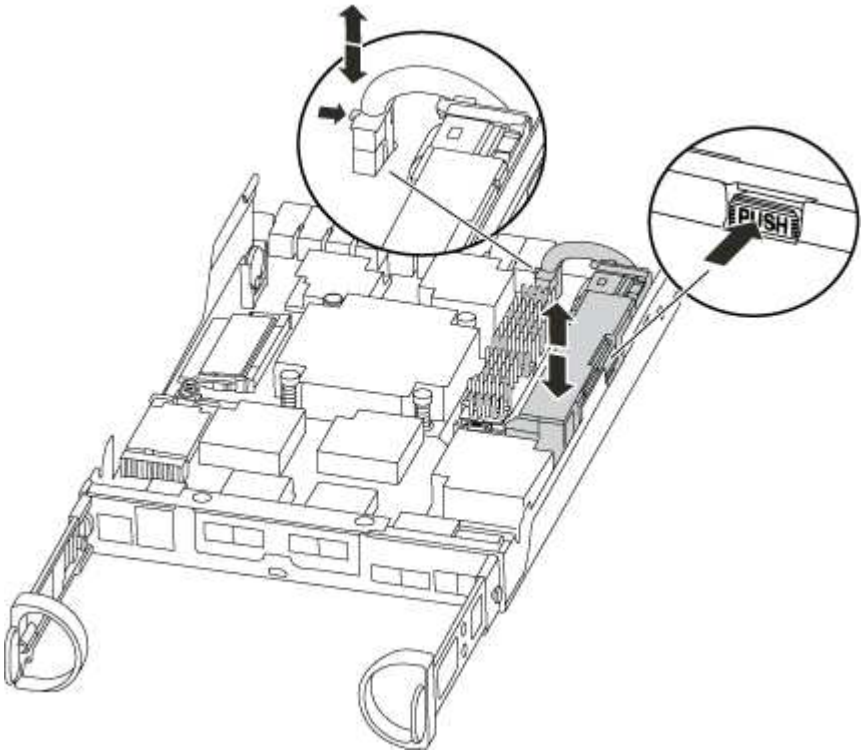
1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Locate the NVMEM battery in the controller module.




3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
4. Remove the battery from the controller module and set it aside.
5. Remove the replacement battery from its package.
6. Loop the battery cable around the cable channel on the side of the battery holder.
7. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.

8. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
9. Plug the battery plug back into the controller module.

#### Step 4: Reinstall the controller module

After you replace components in the controller module, reinstall it into the chassis.

1. If you have not already done so, replace the cover on the controller module.
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. Complete the reinstallation of the controller module:

| If your system is in… | Then perform these steps… |
| --- | --- |
| An HA pair | The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.<br><br>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.<br><br>ⓘ Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br><br>The controller begins to boot as soon as it is seated in the chassis.<br><br>b. If you have not already done so, reinstall the cable management device.<br><br>c. Bind the cables to the cable management device with the hook and loop strap.<br><br>d. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process.<br><br>ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br><br>e. Select the option to boot to Maintenance mode from the displayed menu. |

| If your system is in… | Then perform these steps… |
| --- | --- |
| A stand-alone configuration | 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.<br><br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br><br>b. If you have not already done so, reinstall the cable management device.<br><br>c. Bind the cables to the cable management device with the hook and loop strap.<br><br>d. Reconnect the power cables to the power supplies and to the power sources, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message.<br><br>If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br><br>e. From the boot menu, select the option for Maintenance mode. |

#### Step 5: Run system-level diagnostics

After installing a new NVMEM battery, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the NVMEM memory: `sldiag device run -dev nvmem`
4. Verify that no hardware problems resulted from the replacement of the NVMEM battery: `sldiag device status -dev nvmem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

| If the system-level diagnostics tests… | Then… |
|---|---|
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>SLDIAG: No log messages are present.<br>c. Exit Maintenance mode: `halt`<br>The controller displays the LOADER prompt.<br>d. Boot the controller from the LOADER prompt: `bye`<br>e. Return the controller to normal operation: |

| If your controller is in… | Then… |
|---|---|
| An HA pair | Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`*<br>If you disabled automatic giveback, re-enable it with the storage failover modify command. |
| A stand-alone configuration | Proceed to the next step.<br>No action is required.<br>You have completed system-level diagnostics. |

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

#### 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 & Replacements page for further information.

### Swap out a power supply - FAS2600

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.

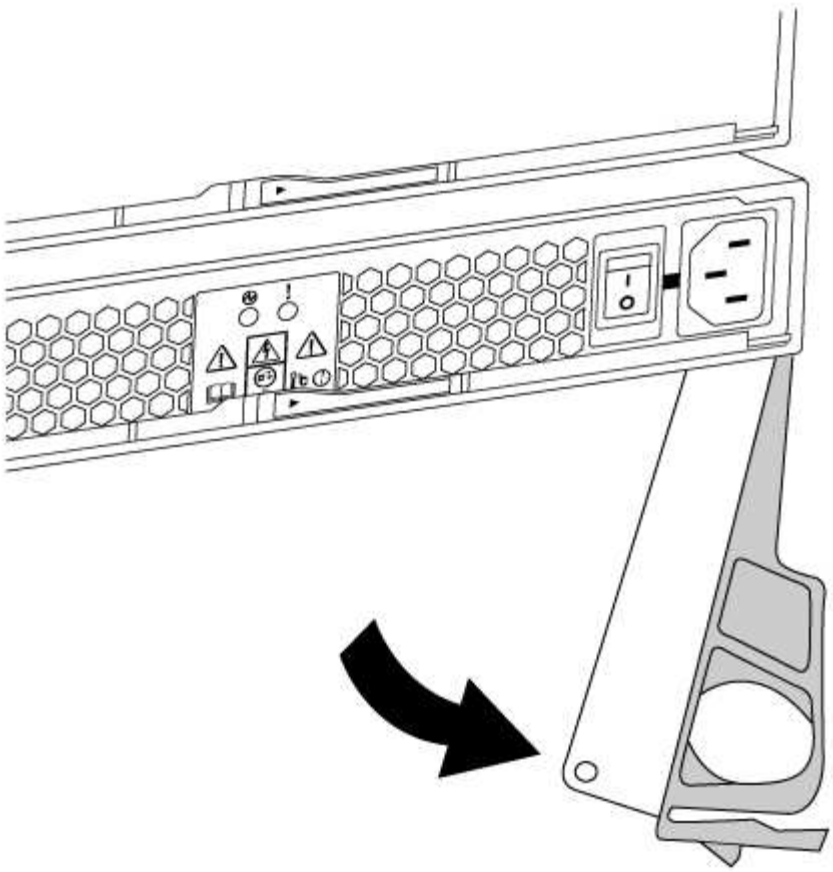
- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> Cooling is integrated with the power supply, so you must replace the power supply within two minutes of removal to prevent overheating due to reduced airflow. Because the chassis provides a shared cooling configuration for the two HA nodes, a delay longer than two minutes will shut down all controller modules in the chassis. If both controller modules do shut down, make sure that both power supplies are inserted, turn both off for 30 seconds, and then turn both on.

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

AFF FAS2600 power supply replacement video

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. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.



5. Use the cam handle to slide the power supply out of the system.

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

6. Make sure that the on/off switch of the new power supply is in the Off position.
7. 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 using the cam handle.

   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.

8. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
9. 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.

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

    The power supply LEDs are lit when the power supply comes online.

11. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Replace the real-time clock battery

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.

AFF FAS2600 RTC battery replacement video

#### Step 1: Shut down the impaired controller

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 the Administration overview with the CLI.

**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_down_h`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. If the impaired controller is part of an HA pair, 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 Remove controller module.. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y`. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br>+<br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

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

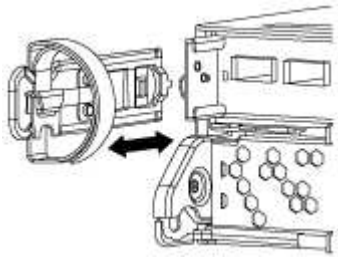
#### Step 2: Remove controller module

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.

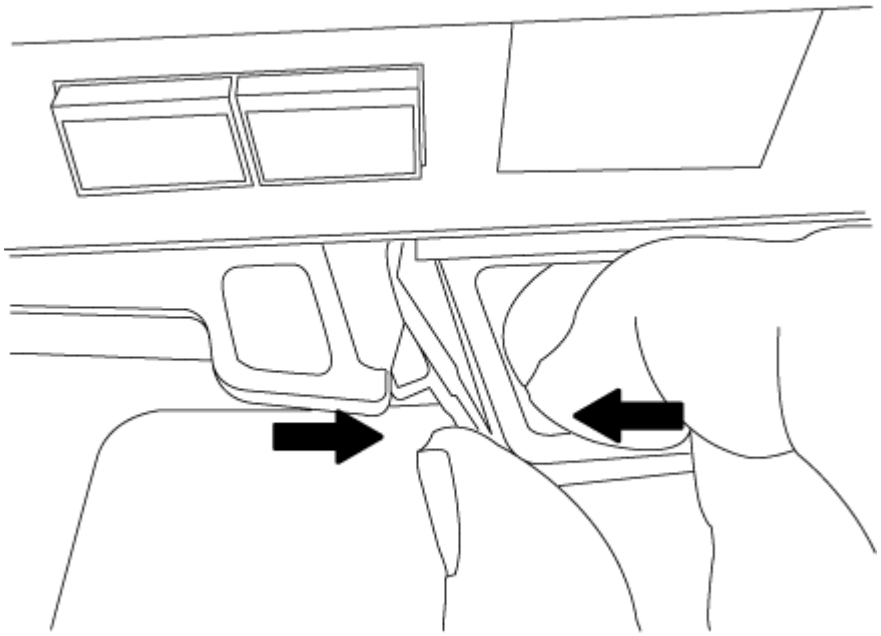
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

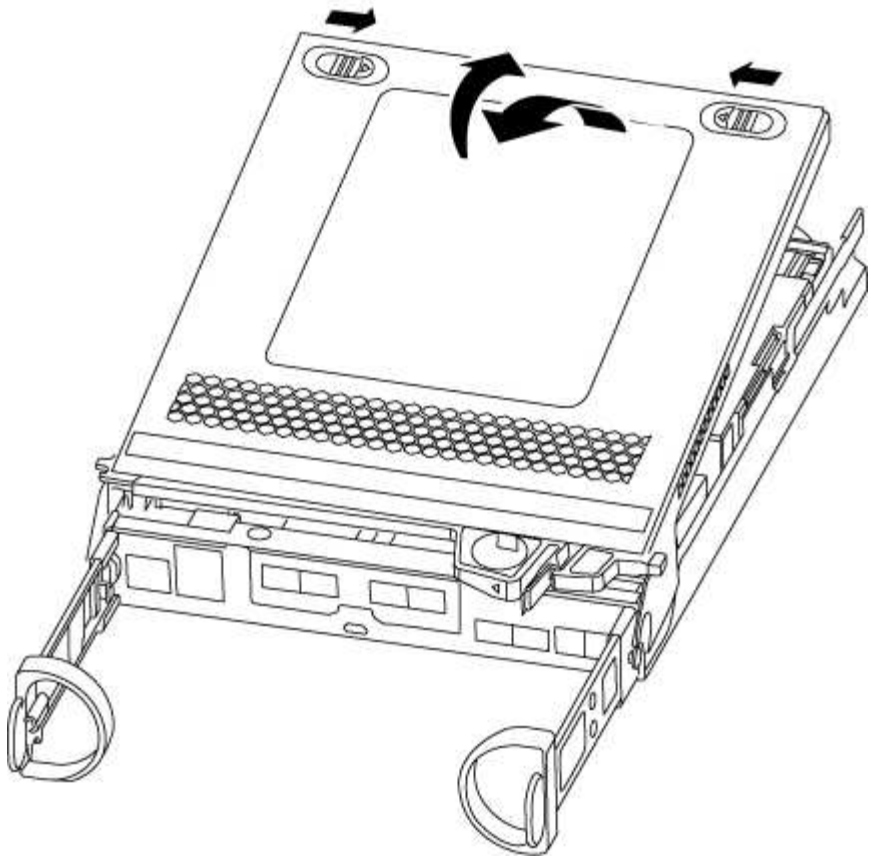
3. Remove and set aside the cable management devices from the left and right sides of the controller module.



4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



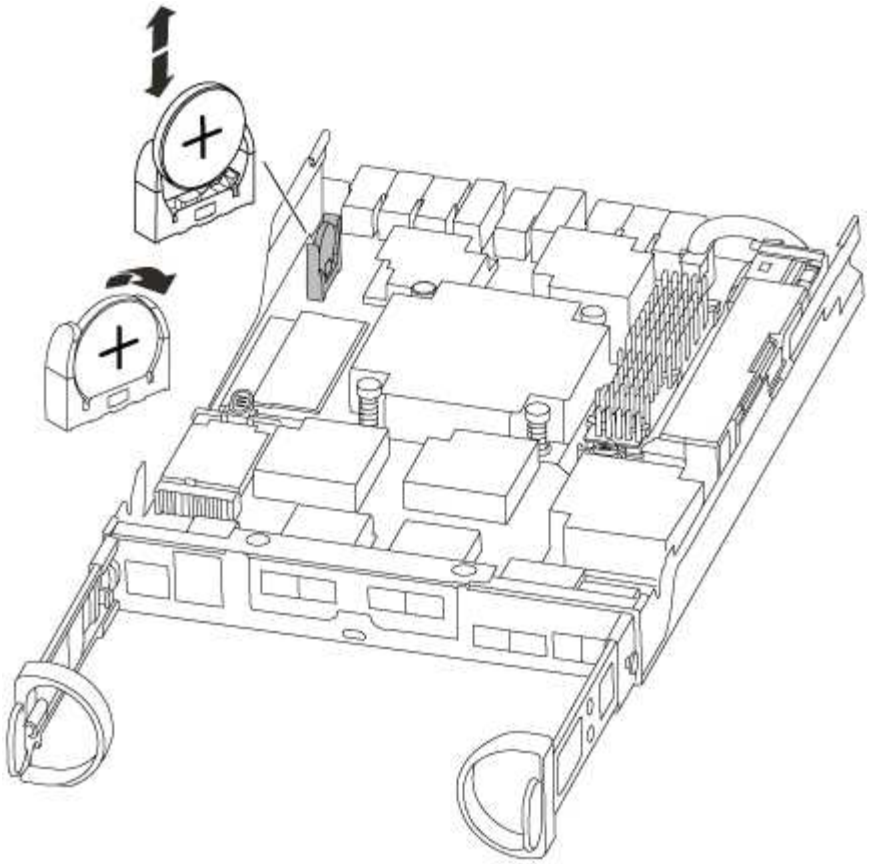
5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.



**Step 3: Replace the RTC battery**

To replace the RTC battery, locate it inside the controller and follow the specific sequence of steps.

1. Locate the RTC battery.



2. 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.

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

#### Step 4: Reinstall the controller module and set time/date after RTC battery replacement

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.

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 controller with the `show date` command.
   b. At the LOADER prompt on the target controller, 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 controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller 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: Complete the replacement process

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

# FAS2700 System Documentation

## Install and setup

### Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

If your system is in a MetroCluster IP configuration, see the Install MetroCluster IP Configuration instructions.

#### Quick guide - AFF A220 and FAS2700

This guide gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

AFF A220/FAS2700 Systems Installation and Setup Instructions

#### Videos - AFF A220 and FAS2700

There are two videos; one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

##### Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

NetApp video: AFF A220 and FAS2700 Systems: Installation and Setup Instructions

##### Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

#### Detailed guide - AFF A220 and FAS2700

This guide gives detailed step-by-step instructions for installing a typical NetApp system. Use this guide if you want more detailed installation instructions.

##### Step 1: Prepare for installation

To install your FAS2700 or AFF A220 system, you need to create an account on the NetApp Support Site, register your system, and get license keys. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

You need to have access to the Hardware Universe for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for

your version of ONTAP for more information about this system.

NetApp Hardware Universe

Find the Release Notes for your version of ONTAP 9

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser
- A laptop or console with an RJ-45 connection and access to a Web browser

**Steps**

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Set up your account:
   a. Log in to your existing account or create an account.
   b. Register your system.

      NetApp Product Registration

4. Download and install Config Advisor on your laptop.

   NetApp Downloads: Config Advisor

5. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the Hardware Universe to locate the cable and identify its use.

   NetApp Hardware Universe

| Type of cable… | Part number and length | Connector type | For… |
|---|---|---|---|
| 10 GbE cable (order dependent) | X6566B-05-R6 (112-00297), 0.5m<br><br>X6566B-2-R6 (112-00299), 2m | | Cluster interconnect network |
| 10 GbE cable (order dependent) | Part number X6566B-2-R6 (112-00299), 2m<br><br>or X6566B-3-R6 (112-00300), 3m<br><br>X6566B-5-R6 (112-00301), 5m | | Data |

| Type of cable… | Part number and length | Connector type | For… |
|---|---|---|---|
| Optical network cables (order dependent) | X6553-R6 (112-00188), 2m<br><br>X6536-R6 (112-00090), 5m<br><br>X6554-R6(112-00189), 15m | | FC host network |
| Cat 6, RJ-45 (order dependent) | Part numbers X6585-R6 (112-00291), 3m<br><br>X6562-R6 (112-00196), 5m | | Management network and Ethernet data |
| Storage (order dependent) | Part number X66030A (112-00435), 0.5m<br><br>X66031A (112-00436), 1m<br><br>X66032A (112-00437), 2m<br><br>X66033A (112-00438), 3m | | Storage |
| Micro-USB console cable | Not applicable | | Console connection during software setup on non-Windows or Mac laptop/console |
| Power cables | Not applicable | | Powering up the system |

6. Download and complete the *Cluster configuration worksheet*.

   Cluster Configuration Worksheet

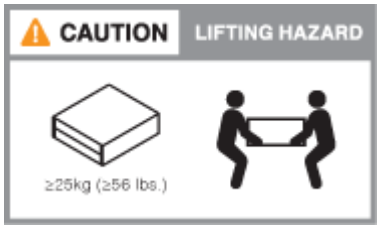
#### Step 2: Install the hardware

## You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

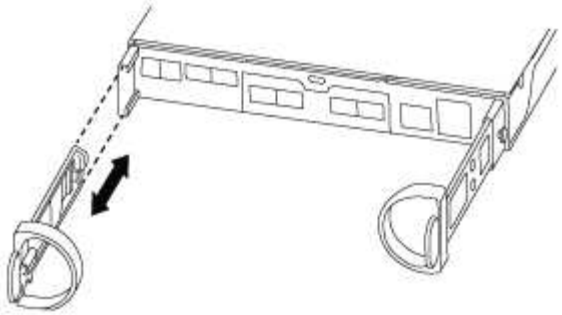
**Steps**

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

   You need to be aware of the safety concerns associated with the weight of the system.




3. Attach cable management devices (as shown).



4. Place the bezel on the front of the system.

#### Step 3: Cable controllers to your network

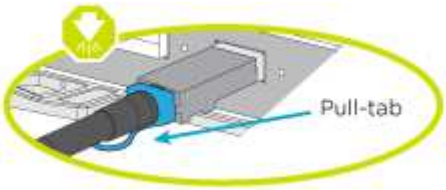
## You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

#### Option 1: Cable a two-node switchless cluster, unified network configuration

## Management network, UTA2 data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled on both controllers.

You must have contacted your network administrator for information about connecting the system to the switches.

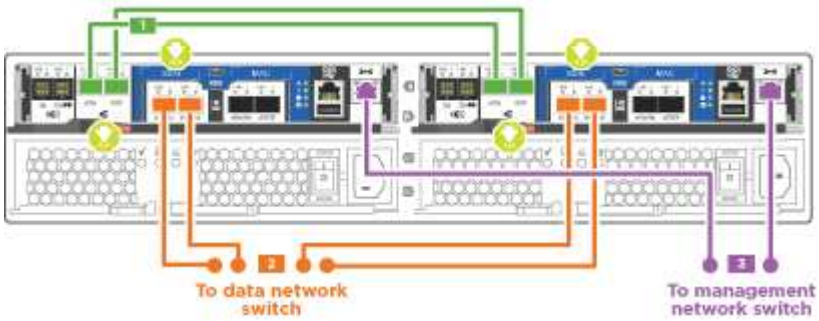
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

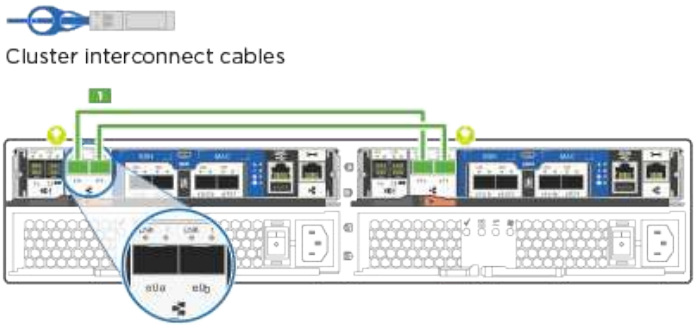
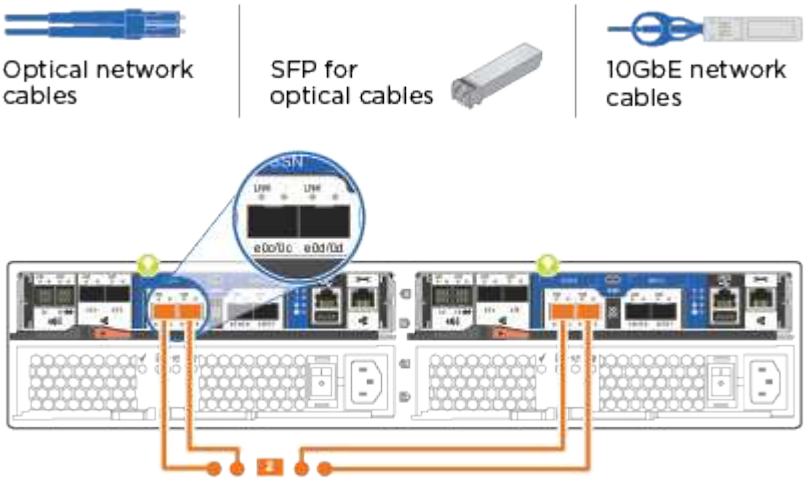


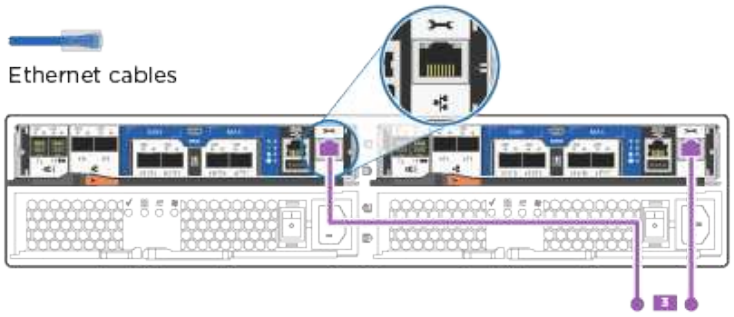

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and to the switches:



| Step | Perform on each controller |
|---|---|
| 1 | Cable the cluster interconnect ports to each other with the cluster interconnect cable:<br><br>• e0a to e0a<br>• e0b to e0b<br><br>  <br> |
| 2 | Use one of the following cable types to cable the UTA2 data ports to your host network:<br><br>An FC host<br><br>• 0c and 0d<br>• **or** 0e and 0f<br>A 10GbE<br>• e0c and e0d<br>• **or** e0e and e0f<br><br>ⓘ You can connect one port pair as CNA and one port pair as FC, or you can connect both port pairs as CNA or both port pairs as FC.<br><br>  <br> |

| Step | Perform on each controller |
| --- | --- |
| 3 | Cable the e0M ports to the management network switches with the RJ45 cables:   |
| ! | DO NOT plug in the power cords at this point. |

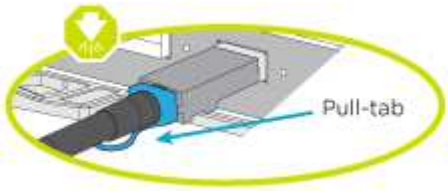
2. To cable your storage, see Cabling controllers to drive shelves

**Option 2: Cable a switched cluster, unified network configuration**

## Management network, UTA2 data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled to the cluster interconnect switches.

You must have contacted your network administrator for information about connecting the system to the switches.

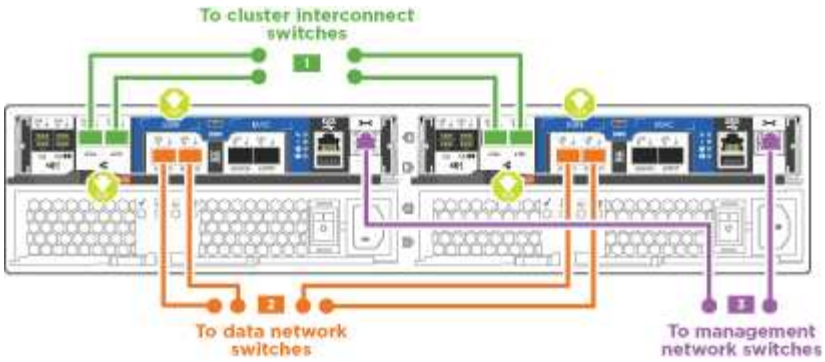
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

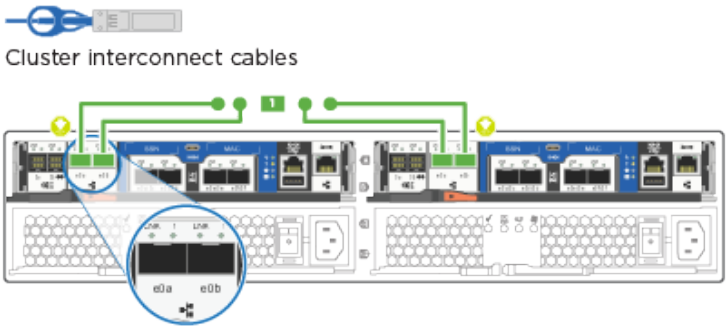


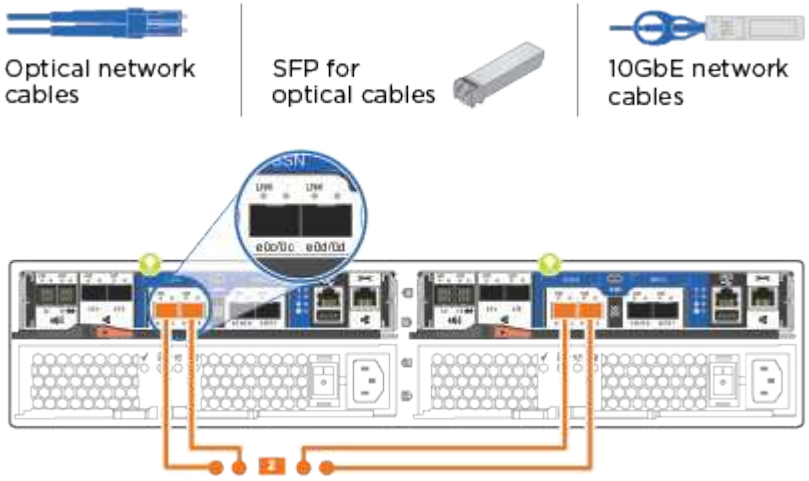
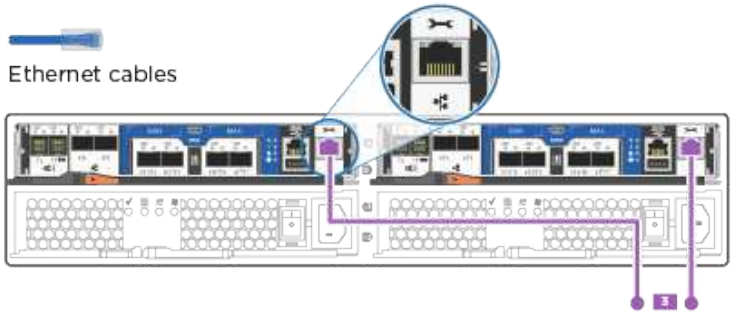

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and the switches:




| Step | Perform on each controller module |
|---|---|
| 1 | Cable e0a and e0b to the cluster interconnect switches with the cluster interconnect cable:<br>  <br> |

| Step | Perform on each controller module |
|---|---|
| 2 | Use one of the following cable types to cable the UTA2 data ports to your host network:<br><br>An FC host<br><br>• 0c and 0d<br>• **or** 0e and 0f<br><br>A 10GbE<br><br>• e0c and e0d<br>• **or** e0e and e0f<br><br>You can connect one port pair as CNA and one port pair as FC, or you can connect both port pairs as CNA or both port pairs as FC.<br><br>  <br> |
| 3 | Cable the e0M ports to the management network switches with the RJ45 cables:<br><br>  <br> |

| Step | Perform on each controller module |
| --- | --- |
| ! | DO NOT plug in the power cords at this point. |

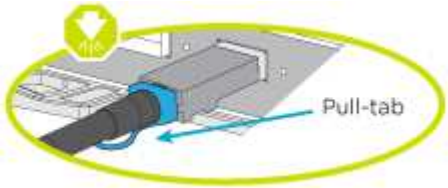
2. To cable your storage, see Cabling controllers to drive shelves

**Option 3: Cable a two-node switchless cluster, Ethernet network configuration**

Management network, Ethernet data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled on both controllers.

You must have contacted your network administrator for information about connecting the system to the switches.

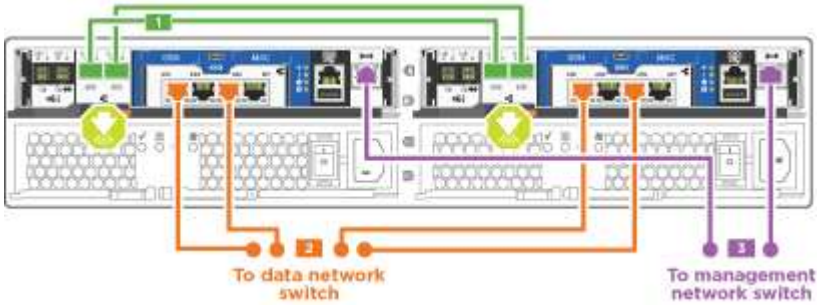
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

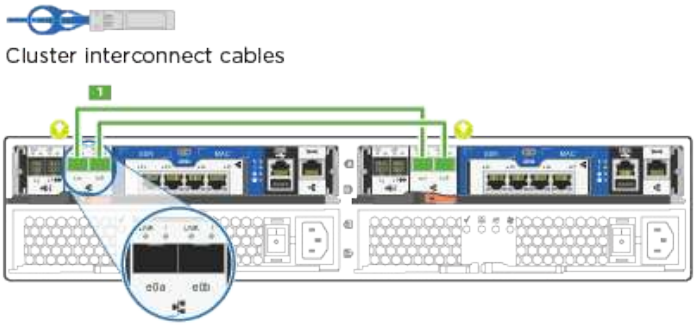
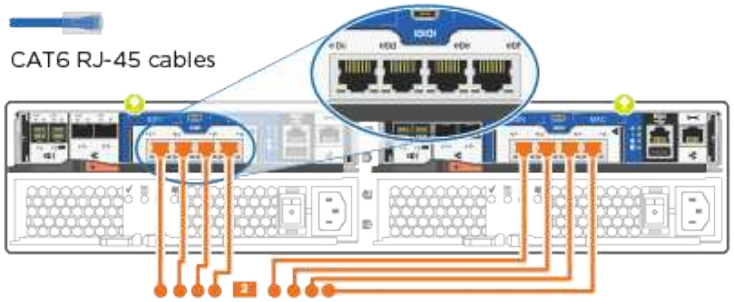
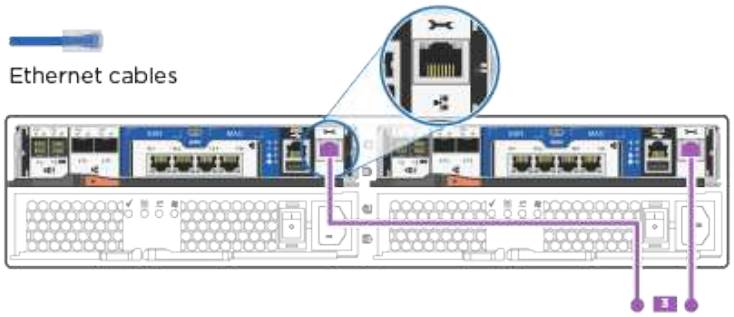



As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and to the switches:



| Step | Perform on each controller |
| --- | --- |
| 1 | Cable the cluster interconnect ports to each other with the cluster interconnect cable:<br>• e0a to e0a<br>• e0b to e0b<br>  |
| 2 | Use the Cat 6 RJ45 cable to cable the e0c through e0f ports to your host network:<br>  |
| 3 | Cable the e0M ports to the management network switches with the RJ45 cables:<br>  |
| ! | DO NOT plug in the power cords at this point. |

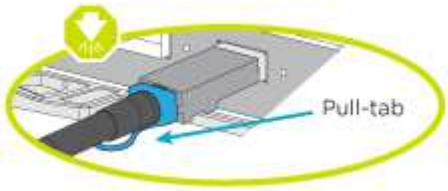
2. To cable your storage, see Cabling controllers to drive shelves

**Option 4: Cable a switched cluster, Ethernet network configuration**

## Management network, Ethernet data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled to the cluster interconnect switches.

You must have contacted your network administrator for information about connecting the system to the switches.

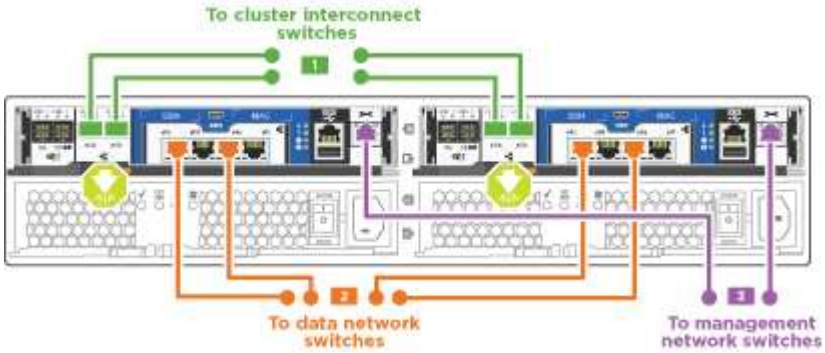
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

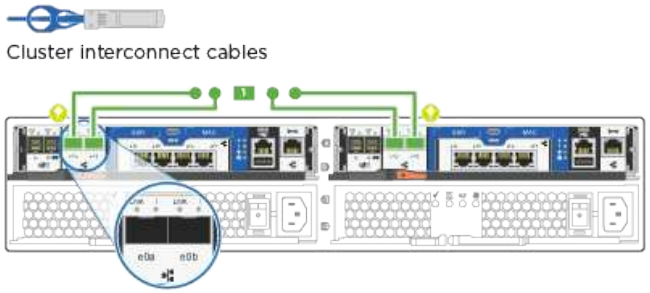
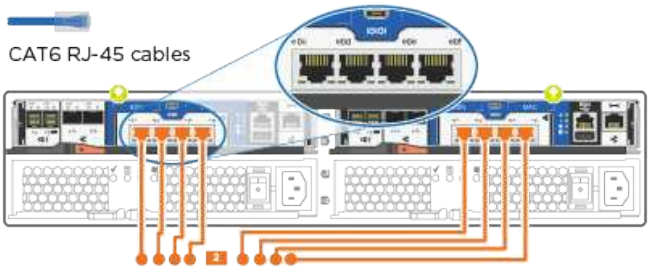
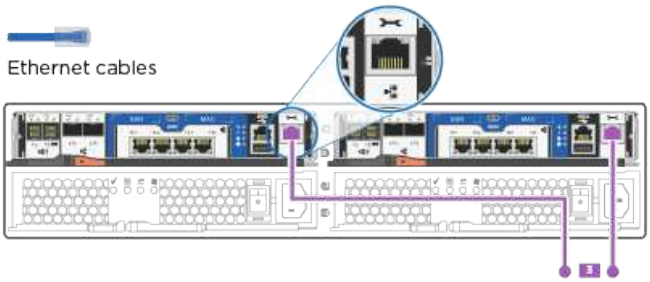



> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. You can use the graphic or the step-by step instructions to complete the cabling between the controllers and the switches:



| Step | Perform on each controller module |
|---|---|
| 1 | Cable e0a and e0b to the cluster interconnect switches with the cluster interconnect cable:   |
| 2 | Use the Cat 6 RJ45 cable to cable the e0c through e0f ports to your host network:   |
| 3 | Cable the e0M ports to the management network switches with the RJ45 cables:   |
| ! | DO NOT plug in the power cords at this point. |

2. To cable your storage, see Cabling controllers to drive shelves

#### Step 4: Cable controllers to drive shelves

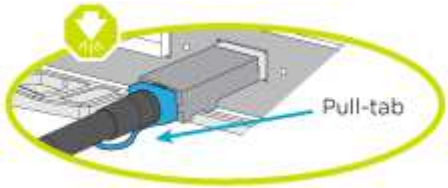
You must cable the controllers to your shelves using the onboard storage ports. NetApp recommends MP-HA cabling for systems with external storage. If you have a SAS tape

drive, you can use single-path cabling. If you have no external shelves, MP-HA cabling to internal drives is optional (not shown) if the SAS cables are ordered with the system.

#### Option 1: Cable storage on an HA pair with external drive shelves

You must cable the shelf-to-shelf connections, and then cable both controllers to the drive shelves.

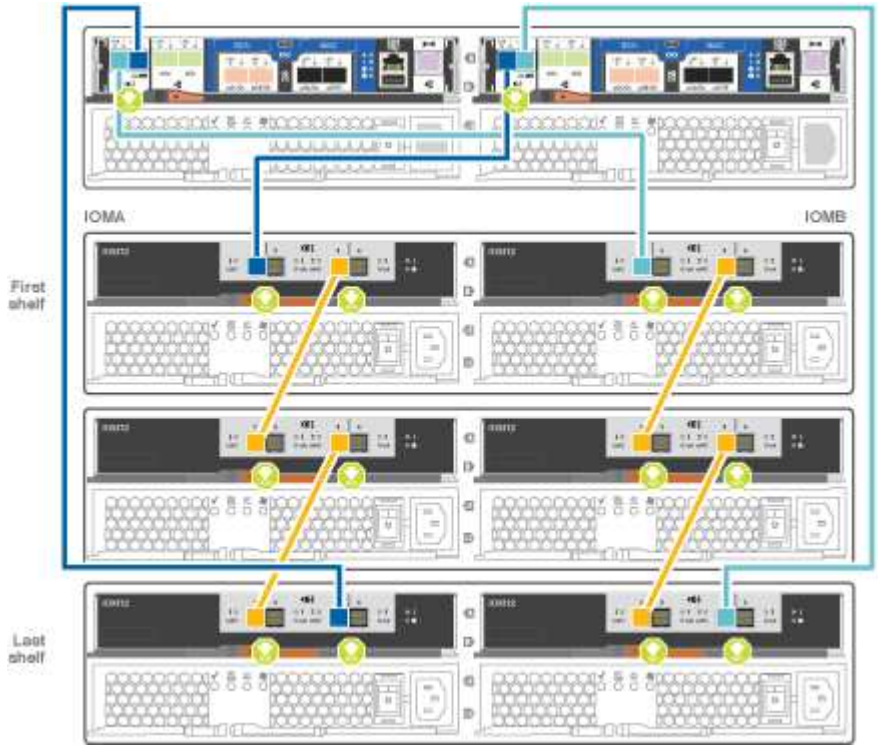
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.




**Steps**

1. Cable the HA pair with external drive shelves:

   The example uses DS224C. Cabling is similar with other supported drive shelves.



| Step | Perform on each controller |
| --- | --- |
| 1 | Cable the shelf-to-shelf ports.<br>• Port 3 on IOM A to port 1 on the IOM A on the shelf directly below.<br>• Port 3 on IOM B to port 1 on the IOM B on the shelf directly below.<br>mini-SAS HD to mini-SAS HD cables |
| 2 | Connect each node to IOM A in the stack.<br>• Controller 1 port 0b to IOM A port 3 on last drive shelf in the stack.<br>• Controller 2 port 0a to IOM A port 1 on the first drive shelf in the stack.<br>mini-SAS HD to mini-SAS HD cables |
| 3 | Connect each node to IOM B in the stack<br>• Controller 1 port 0a to IOM B port 1 on first drive shelf in the stack.<br>• Controller 2 port 0b to IOM B port 3 on the last drive shelf in the stack.<br>mini-SAS HD to mini-SAS HD cables |

If you have more than one drive shelf stack, see the *Installation and Cabling Guide* for your drive shelf type.

Installing and cabling

2. To complete setting up your system, see Completing system setup and configuration

#### Step 5: Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

#### Option 1: Complete system setup if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

**Steps**

1. Use the following animation to set one or more drive shelf IDs

   Setting drive shelf IDs

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Turn on the power switches to both nodes.

Initial booting may take up to eight minutes.

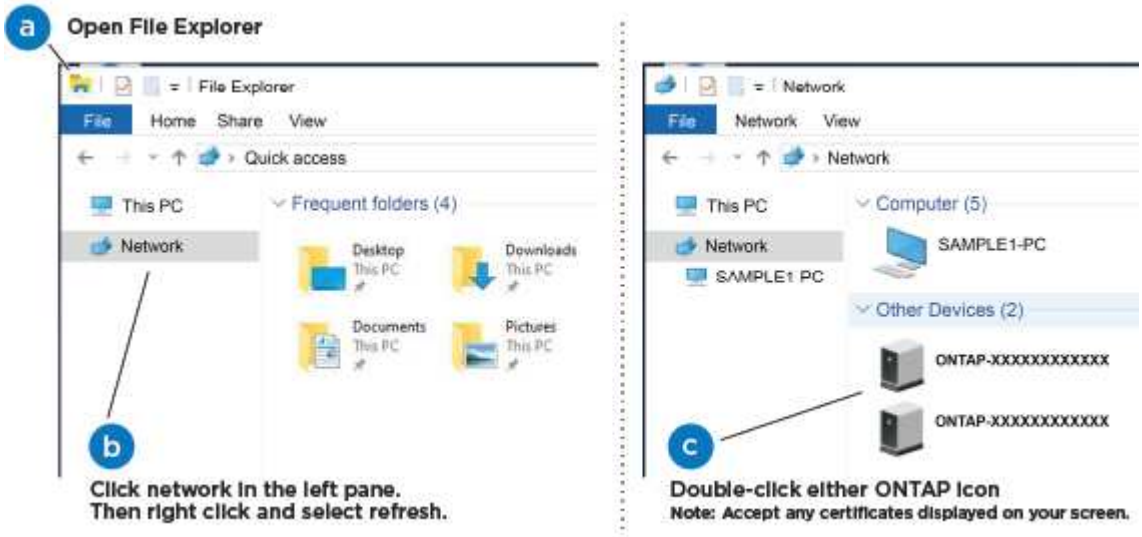
4. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

5. Use the following animation to connect your laptop to the Management switch.

   Connecting your laptop to the Management switch

6. Select an ONTAP icon listed to discover:




   a. Open File Explorer.
   b. Click network in the left pane.
   c. Right click and select refresh.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

   XXXXX is the system serial number for the target node.

   System Manager opens.

7. Use System Manager guided setup to configure your system using the data you collected in the *NetApp ONTAP Configuration Guide*.

   ONTAP Configuration Guide

8. Verify the health of your system by running Config Advisor.
9. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

**Option 2: Completing system setup and configuration if network discovery is not enabled**

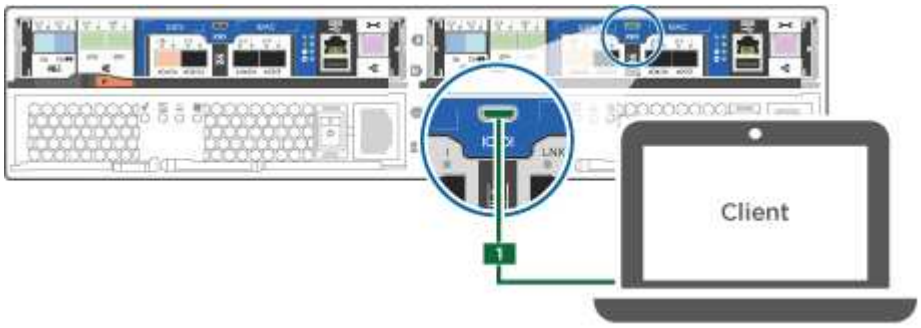
If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

**Steps**

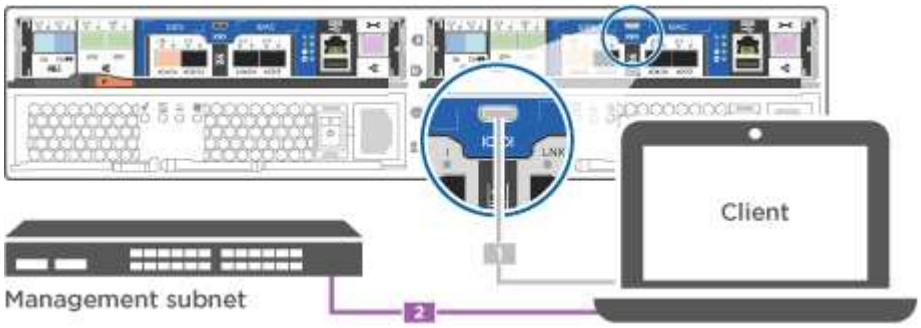
1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

      See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console, and connect the console port on the controller using the console cable that came with your system.




   c. Connect the laptop or console to the switch on the management subnet.




   d. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.
2. Use the following animation to set one or more drive shelf IDs:

   Setting drive shelf IDs

3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
4. Turn on the power switches to both nodes.

Initial booting may take up to eight minutes.

5. Assign an initial node management IP address to one of the nodes.

| If the management network has DHCP… | Then… |
|---|---|
| Configured | Record the IP address assigned to the new controllers. |
| Not configured | a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment.<br>Check your laptop or console's online help if you do not know how to configure PuTTY.<br>b. Enter the management IP address when prompted by the script. |

6. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

      The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the *NetApp ONTAP Configuration guide*.

      ONTAP Configuration Guide

7. Verify the health of your system by running Config Advisor.
8. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

## Maintain

### Boot media

#### Overview of boot media replacement - AFF A220 and FAS2700

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` file.

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 must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

#### Check onboard encryption keys - AFF A220 and FAS2700

## Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

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 the NetApp Encryption overview with the CLI.

**Steps**

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. 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`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.

- If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to [Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier].
- If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to [Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later].

4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

#### Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

**Steps**

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

#### Verify NVE configuration

**Steps**

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps.
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers

display `available`: `security key-manager query`

c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes` manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shutdown the controller.

### Verify NSE configuration

#### Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`

   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps

2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:

a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

   If the command fails, contact NetApp Support.

   mysupport.netapp.com

b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to back up the OKM information: `security key-manager backup show`

        Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

      - Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shut down the controller.

**Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later**

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If

so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

**Verify NVE configuration**

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`
     e. Shut down the impaired controller.
  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
     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.

mysupport.netapp.com

b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

### Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back

up the OKM information:

a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

b. Enter the command to display the key management information: `security key-manager onboard show-backup`

c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

d. Return to admin mode: `set -priv admin`

e. You can safely shut down the controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

   c. You can safely shut down the controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

#### Shut down the impaired controller - AFF A220 and FAS2700

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

configuration.

#### Option 1: Most configurations

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 `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name`<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

1. 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 controller.

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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### Replace the boot media - AFF A220 and FAS2700

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.

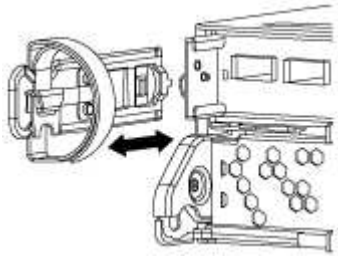
### Step 1: Remove the controller module

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.

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

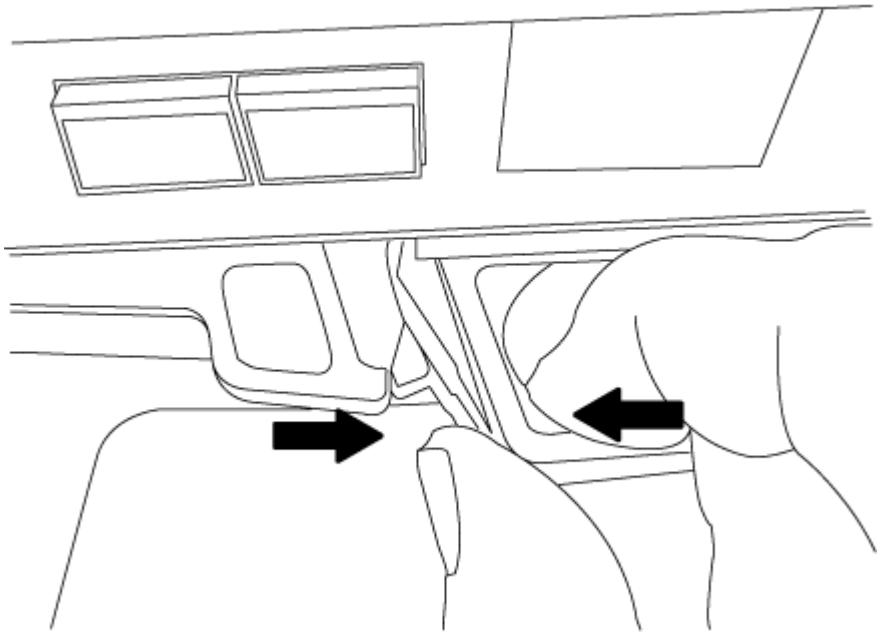
   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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

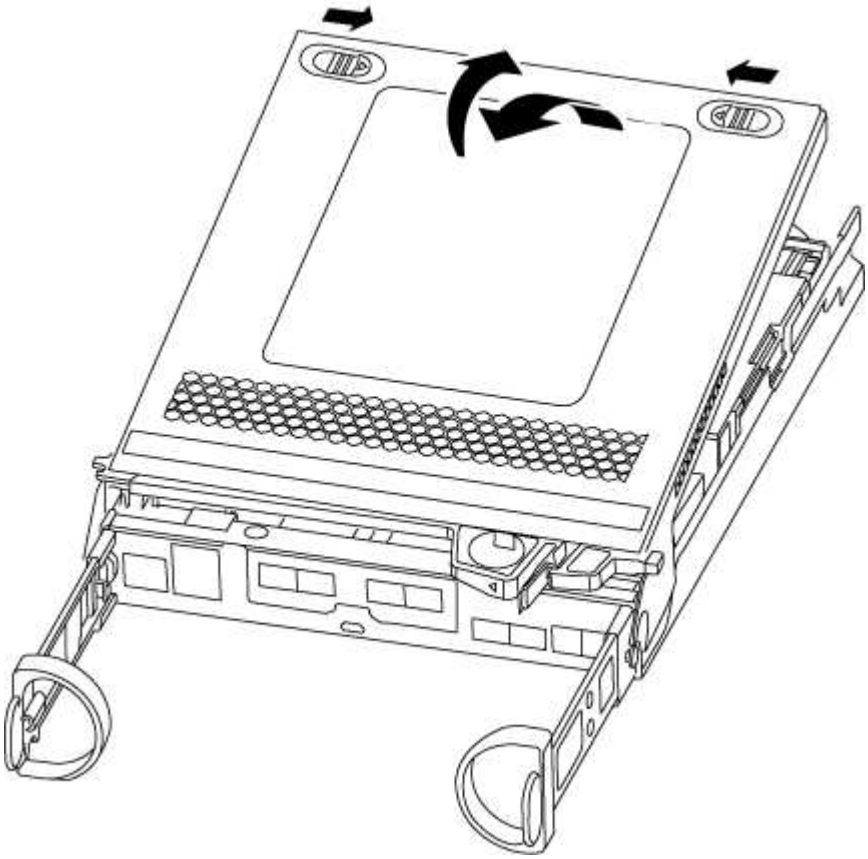


4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller

module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

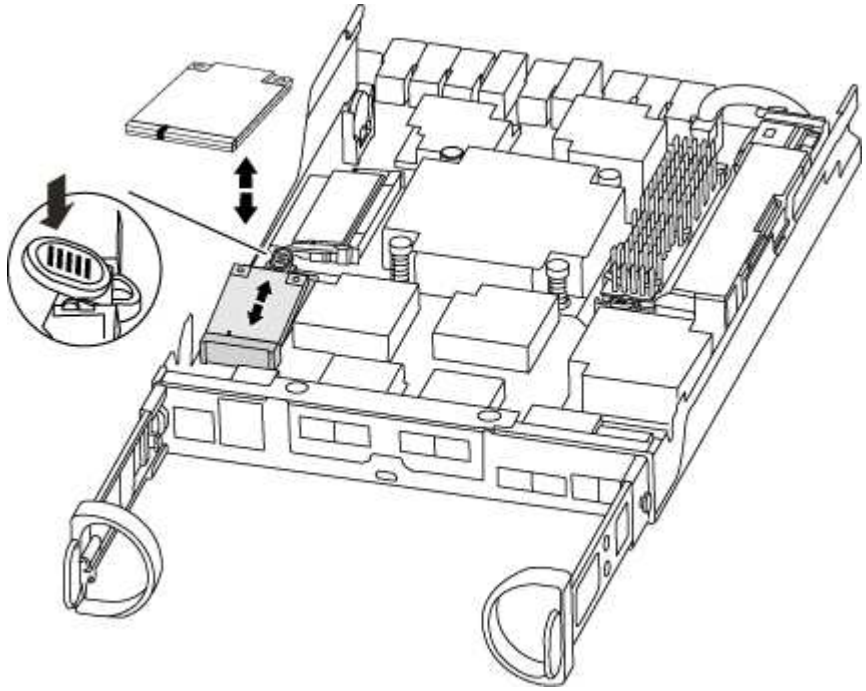


### Step 2: Replace the boot media

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

#### Steps

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



3. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

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

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

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

6. Push the boot media down to engage the locking button on the boot media housing.
7. Close the controller module cover.

### 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 an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

**Steps**

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs) if they were removed.

3. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, push the cam handle to the closed position, and then tighten the thumbscrew.

   The controller 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 controller to boot to LOADER.

6. For systems with one controller in the chassis, reconnect the power and turn on the power supplies.

   The system begins to boot and stops at the LOADER prompt.

7. 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 controller from the healthy controller 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.

#### Boot the recovery image - AFF A220 and FAS2700

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

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

4. Ensure that the environmental variables are set as expected:

a. Take the controller 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 controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

7. Connect the console cable to the partner controller.

8. Give back the controller 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 controller 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.

#### Restore OKM, NSE, and NVE as needed - AFF A220 and FAS2700

## Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.

- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

### Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

#### Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
|---|---|
| The LOADER prompt | Boot the controller to the boot menu: `boot_ontap menu` |
| Waiting for giveback… | a. Enter `Ctrl-C` at the prompt<br>b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y`<br>c. At the LOADER prompt, enter the `boot_ontap menu` command. |

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

   > The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:

```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.
9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      > Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.

b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

> If the `Restored` column = anything other than `yes`, contact Customer Support.

c. Wait 10 minutes for the key to synchronize across the cluster.

14. If you are running ONTAP 9.6 or later:

    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.

    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

    > If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.

15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

### Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

#### Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
|---|---|
| The login prompt | Go to Step 7. |

| If the console displays… | Then… |
| --- | --- |
| Waiting for giveback… | a. Log into the partner controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

      Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.
12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

### Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

**Steps**

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
|---|---|
| The login prompt | Go to Step 7. |
| Waiting for giveback… | a. Log into the partner controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.
   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.

5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

    - If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

      Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

#### Return the failed part to NetApp - AFF A220 and FAS2700

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

#### Replace the caching module - AFF A220 and FAS2700

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation.

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

#### Step 1: Shut down the impaired controller

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 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.

+
ONTAP 9 System Administration Reference

You might want to erase the contents of your caching module before replacing it.

**Steps**

1. Although data on the caching module is encrypted, you might want to erase any data from the impaired caching module and verify that the caching module has no data:
   a. Erase the data on the caching module: `system controller flash-cache secure-erase run`
   b. Verify that the data has been erased from the caching module: `system controller flash-cache secure-erase show -node node_name`

      The output should display the caching module status as erased.
2. If the impaired controller is part of an HA pair, 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 `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller:<br>• For an HA pair, take over the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`.<br>• For a stand-alone system: `system node halt` *`impaired_node_name`* |

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

#### Step 2: Remove controller module

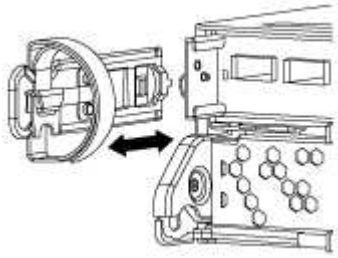
To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

**Steps**

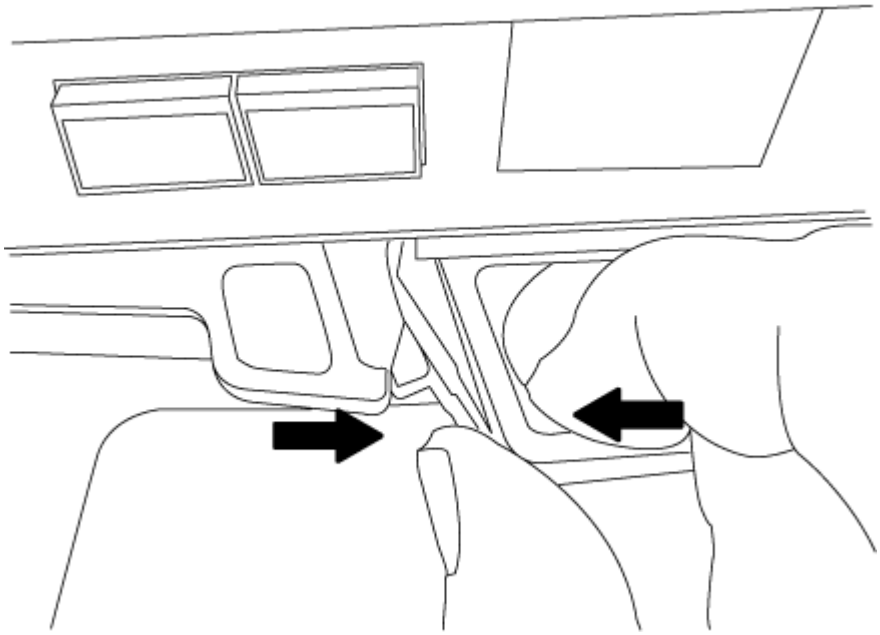
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

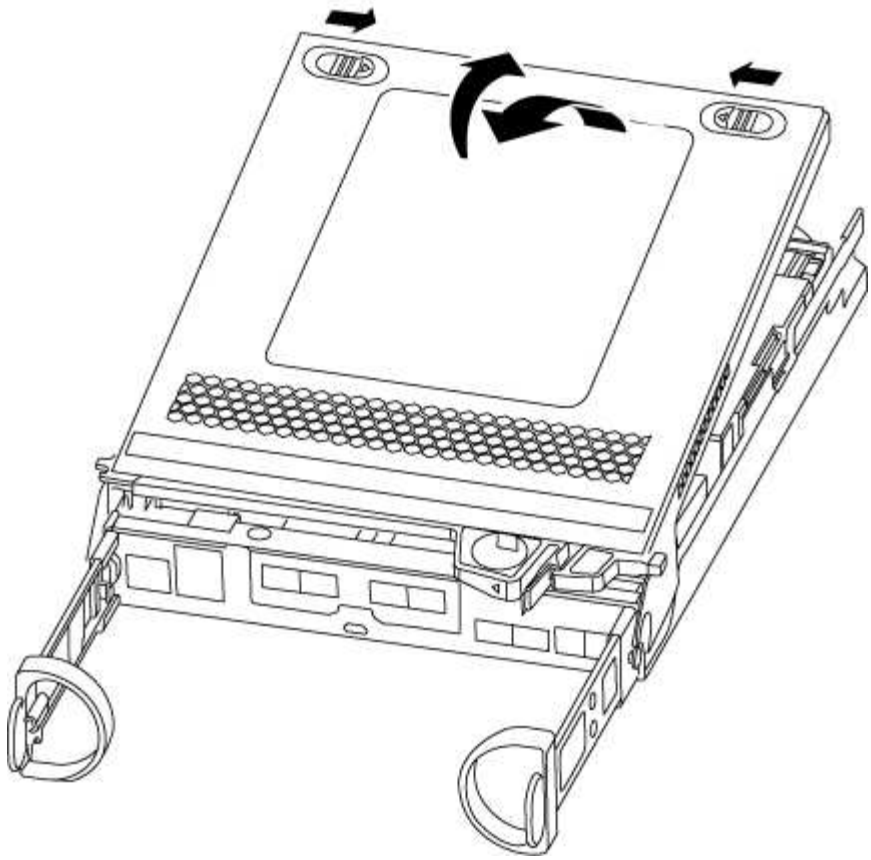
3. Remove and set aside the cable management devices from the left and right sides of the controller module.



4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.



**Step 3: Replace a caching module**

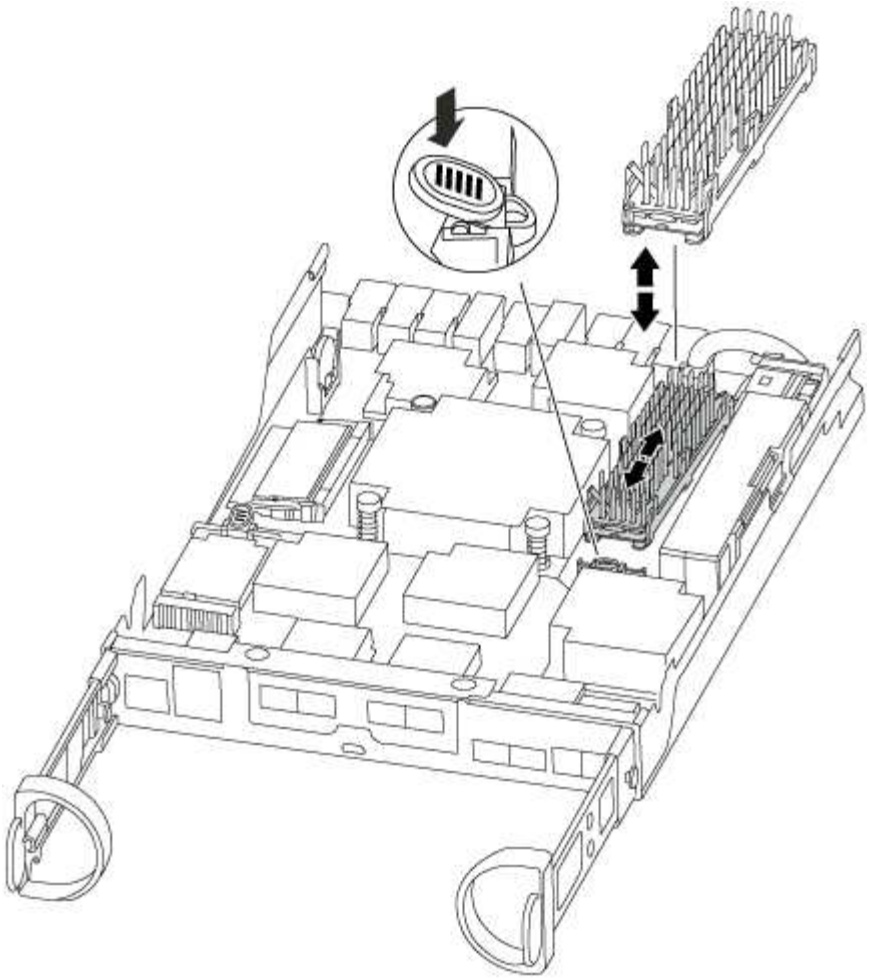
## To replace a caching module referred to as the M.2 PCIe card on the label on your controller, locate the slot inside the controller and follow the specific sequence of steps.

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

**Steps**

1. If you are not already grounded, properly ground yourself.
2. Locate the caching module at the rear of the controller module and remove it.
   a. Press the release tab.
   b. Remove the heatsink.



3. Gently pull the caching module straight out of the housing.
4. Align the edges of the caching module with the socket in the housing, and then gently push it into the socket.
5. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

6. Reseat and push the heatsink down to engage the locking button on the caching module housing.
7. Close the controller module cover, as needed.

#### Step 4: Reinstall the controller module

## After you replace components in the controller module, reinstall it into 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. 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.

5. Complete the reinstallation of the controller module:

| If your system is in… | Then perform these steps… |
|---|---|
| An HA pair | The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.<br><br>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.<br><br>ⓘ Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br><br>The controller begins to boot as soon as it is seated in the chassis.<br><br>b. If you have not already done so, reinstall the cable management device.<br><br>c. Bind the cables to the cable management device with the hook and loop strap.<br><br>d. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process.<br><br>ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br><br>e. Select the option to boot to Maintenance mode from the displayed menu. |

| If your system is in… | Then perform these steps… |
| --- | --- |
| A stand-alone configuration | 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.<br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. Bind the cables to the cable management device with the hook and loop strap.<br>d. Reconnect the power cables to the power supplies and to the power sources, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message.<br>If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br>e. From the boot menu, select the option for Maintenance mode. |

#### Step 5: Run system-level diagnostics

## After installing a new caching module, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

**Steps**

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>)

appears.

3. Run diagnostics on the caching module: `sldiag device run -dev fcache`
4. Verify that no hardware problems resulted from the replacement of the caching module: `sldiag device status -dev fcache -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

1. Proceed based on the result of the preceding step:

| If the system-level diagnostics tests… | Then… |
|---|---|
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br><br>The following default response is displayed:<br><br>SLDIAG: No log messages are present.<br><br>c. Exit Maintenance mode: `halt`<br><br>The controller displays the LOADER prompt.<br><br>d. Boot the controller from the LOADER prompt: `bye`<br>e. Return the controller to normal operation:<br><br>**If your controller is in an HA pair**, perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`*<br><br>**Note:** If you disabled automatic giveback, re-enable it with the `storage failover modify` command.<br><br>**If your controller is in a stand-alone configuration**, proceed to the next step. No action is required.<br><br>You have completed system-level diagnostics. |

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

#### Step 6: Switch back aggregates in a two-node MetroCluster configuration

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

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 7: 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 & Replacements page for further information.

### Chassis

#### Overview of chassis replacement - AFF A220 and FAS2700

To replace the chassis, you must move the power supplies, 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.

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 written with the assumption that you are moving all drives and controller module or modules to the new chassis, and that the chassis is a new component from NetApp.
- This procedure is disruptive. For a two-controller cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

#### Shut down the controllers - AFF A220 and FAS2700

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

#### Option 1: Most configurations

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

#### About this task

- If you have a cluster with more than two controllers, 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 the Administration overview with the CLI.
- 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`

#### Steps

1. If your system has two controller modules, disable the HA pair.

| If your system is running clustered ONTAP with… | Then… |
| --- | --- |
| Two controllers in the cluster | `cluster ha modify -configured false` `storage failover modify -node node0 -enabled false` |
| More than two controllers in the cluster | `storage failover modify -node node0 -enabled false` |

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

#### Option 2: Controller is in a MetroCluster configuration

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 the Administration overview with the CLI.

- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### Move and replace hardware - AFF A220 and FAS2700

## Move the power supplies, 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: Move a power supply

Moving out a power supply when replacing a chassis involves turning off, disconnecting, and removing the power supply from the old chassis and installing and connecting it on the replacement 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. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.

4. Use the cam handle to slide the power supply out of the system.

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

5. Repeat the preceding steps for any remaining power supplies.
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 using the cam handle.

   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. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
8. 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.

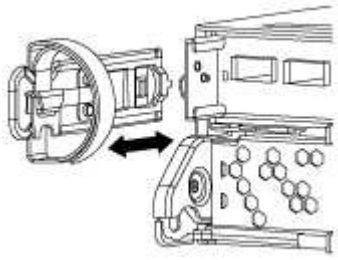
**Step 2: Remove the controller module**

Remove the controller module or modules from the old chassis.

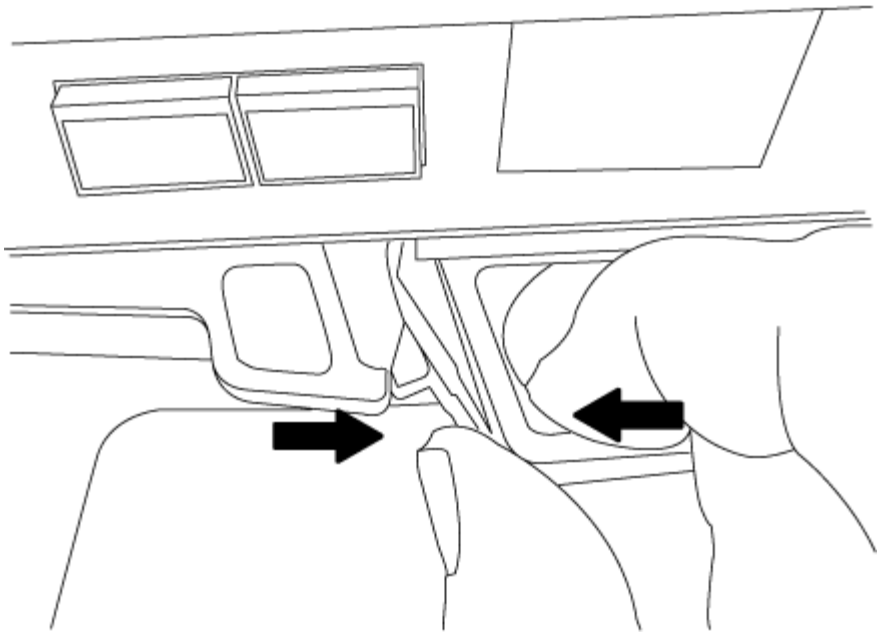
1. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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



3. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module 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 3: Move drives to the new chassis**

You need to move the drives from each bay opening in the old chassis to the same bay opening in the new chassis.

1. Gently remove the bezel from the front of the system.
2. Remove the drives:
   a. Press the release button at the top of the carrier face below the LEDs.
   b. Pull the cam handle to its fully open position to unseat the drive from the midplane, and then gently slide the drive out of the chassis.

      The drive should disengage from the chassis, allowing it to slide free of the chassis.

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

      Drives are fragile. Handle them as little as possible to prevent damage to them.
3. Align the drive from the old chassis with the same bay opening in the new chassis.
4. Gently push the drive into the chassis as far as it will go.

   The cam handle engages and begins to rotate upward.
5. Firmly push the drive the rest of the way into the chassis, and then lock the cam handle by pushing it up and against the drive holder.

   Be sure to close the cam handle slowly so that it aligns correctly with the front of the drive carrier. It click when it is secure.
6. Repeat the process for the remaining drives in the system.

### Step 4: Replace a chassis from within the equipment rack or system cabinet

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.
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. If you have not already done so, install the bezel.

### Step 5: Install the controller

After you install the controller module and any other components into the new chassis, boot it to a state where you can run the interconnect diagnostic test.

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.

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. Repeat the preceding steps if there is a second controller to install in the new chassis.
4. Complete the installation of the controller module:

| If your system is in… | Then perform these steps… |
| --- | --- |
| An HA pair | 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.<br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. Bind the cables to the cable management device with the hook and loop strap.<br>d. Repeat the preceding steps for the second controller module in the new chassis. |
| A stand-alone configuration | 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.<br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. Bind the cables to the cable management device with the hook and loop strap.<br>d. Reinstall the blanking panel and then go to the next step. |

5. Connect the power supplies to different power sources, and then turn them on.
6. Boot each controller to Maintenance mode:
   a. As each controller 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.

#### Restore and verify the configuration - AFF A220 and FAS2700

You must verify the HA state of the chassis and run System-Level diagnostics, switch back aggregates, 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.

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. The next step depends on your system configuration.

| If your system is in… | Then… |
|---|---|
| A stand-alone configuration | a. Exit Maintenance mode: `halt`<br>b. Go to "Completing the replacement process. |
| An HA pair with a second controller module | Exit Maintenance mode: `halt` The LOADER prompt appears. |

### Step 2: Run system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

> During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second controller if you are in an HA configuration.

   > Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

| If the system-level diagnostics tests… | Then… |
| --- | --- |
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br><br>The following default response is displayed:<br><br>`SLDIAG: No log messages are present.`<br><br>c. Exit Maintenance mode on both controllers: `halt`<br><br>The system displays the LOADER prompt.<br><br>You must exit Maintenance mode on both controllers before proceeding any further.<br><br>d. Enter the following command on both controllers at the LOADER prompt: `bye`<br>e. Return the controller to normal operation: |

| If your system is running ONTAP… | Then… |
| --- | --- |
| With two nodes in the cluster | Issue these commands: `node::> cluster ha modify -configured true``node::> storage failover modify -node node0 -enabled true` |
| With more than two nodes in the cluster | Issue this command:`node::> storage failover modify -node node0 -enabled true` |
| In a two-node MetroCluster configuration | Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process. |
| In a stand-alone configuration | You have no further steps in this particular task.<br><br>You have completed system-level diagnostics. |

| If your system is running ONTAP… | Then… |
| --- | --- |
| Resulted in some test failures | Determine the cause of the problem.<br>a. Exit Maintenance mode: `halt`<br>b. Perform a clean shutdown, and then disconnect the power supplies.<br>c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Reconnect the power supplies, and then power on the storage system.<br>e. Rerun the system-level diagnostics test. |

### Step 3: Switch back aggregates in a two-node MetroCluster configuration

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

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 & Replacements page for further information.

### Controller

#### Overview of controller module replacement - AFF A220 and FAS2700

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 is in an HA pair, the healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- 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 controller 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.

- This procedure includes steps for automatically or manually reassigning drives to the *replacement* controller, depending on your system's configuration.

  You should perform the drive reassignment as directed in the procedure.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller 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* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller'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 A220 and FAS2700

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### Replace the controller module hardware - AFF A220 and FAS2700

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

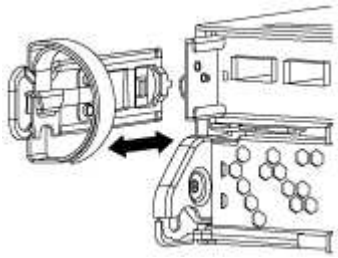
### Step 1: Remove controller module

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

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

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

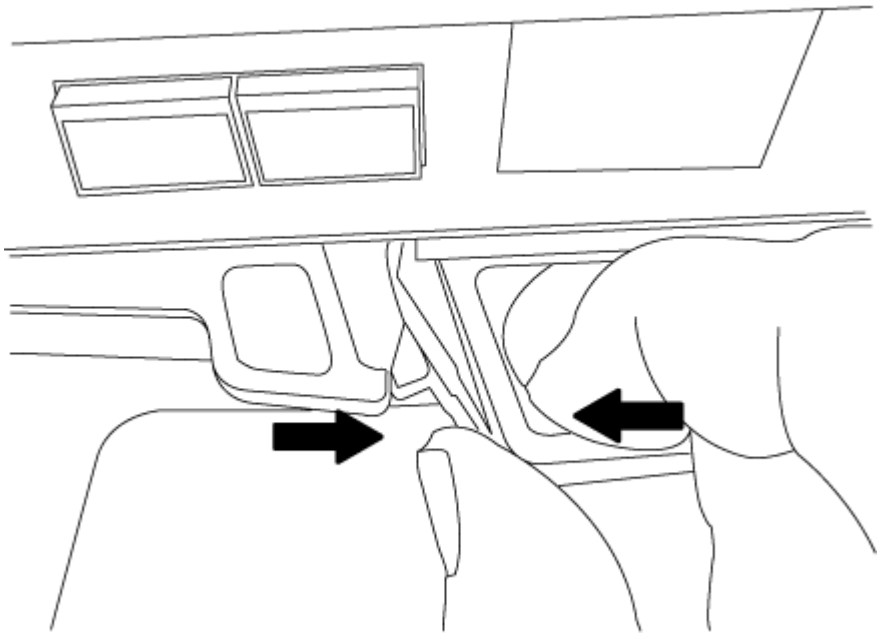
3. Remove and set aside the cable management devices from the left and right sides of the controller module.



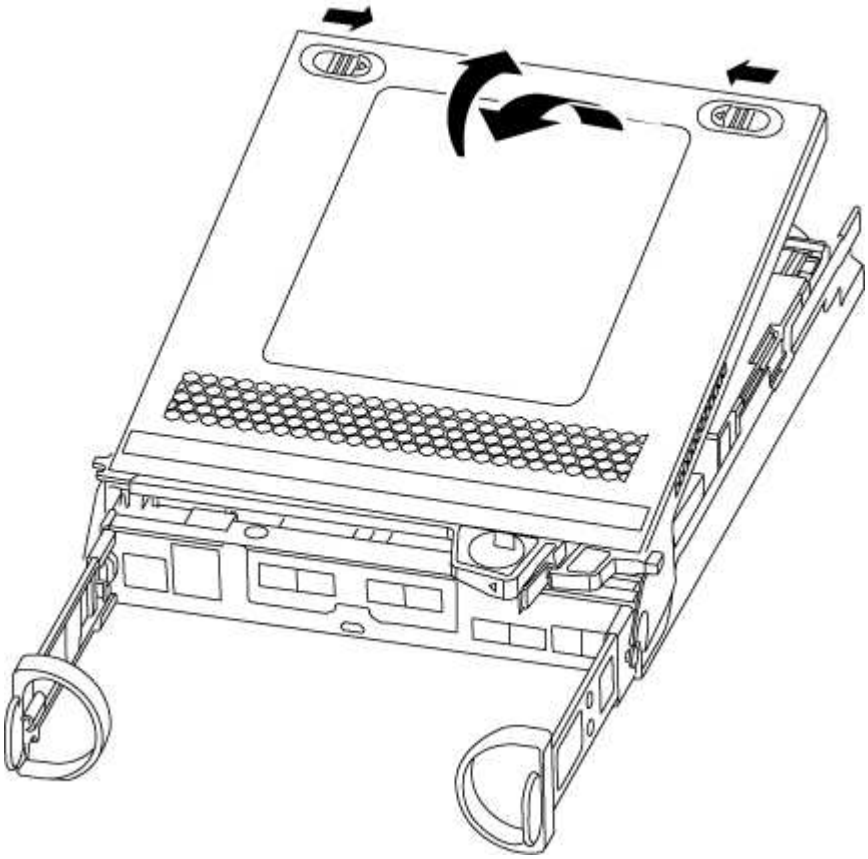
4. If you left the SFP modules in the system after removing the cables, move them to the new controller

module.

5. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



6. Turn the controller module over and place it on a flat, stable surface.
7. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.



**Step 2: Move the NVMEM battery**

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

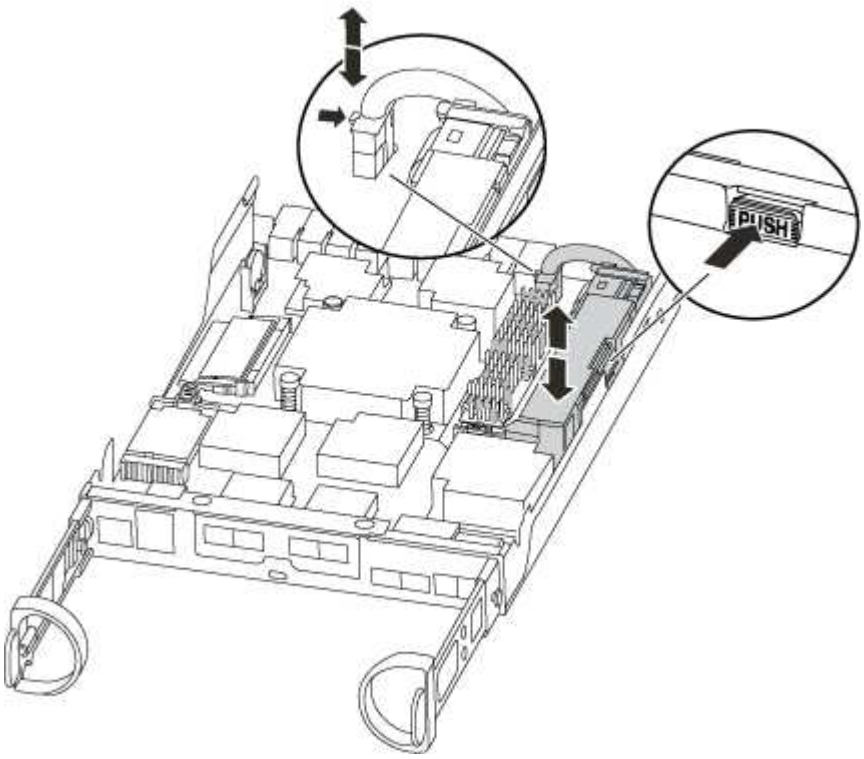
1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

2. Locate the NVMEM battery in the controller module.



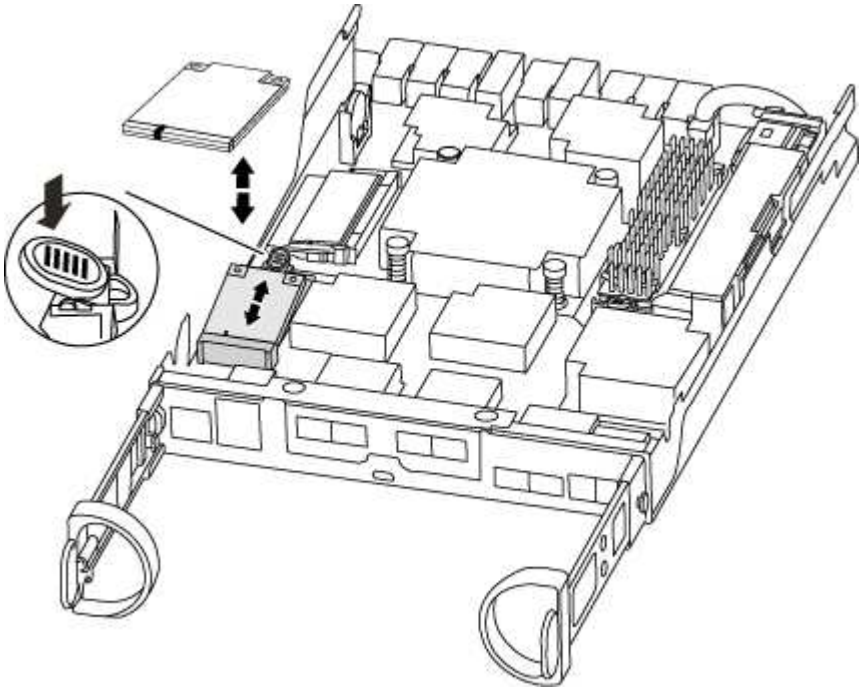

3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.

4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
5. Move the battery to the replacement controller module.
6. Loop the battery cable around the cable channel on the side of the battery holder.
7. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
8. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.

**Step 3: Move the boot media**

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

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



2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

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

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

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

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

### Step 4: Move the DIMMs

To move the DIMMs, you must follow the directions to locate and move them from the old controller module into the replacement controller module.

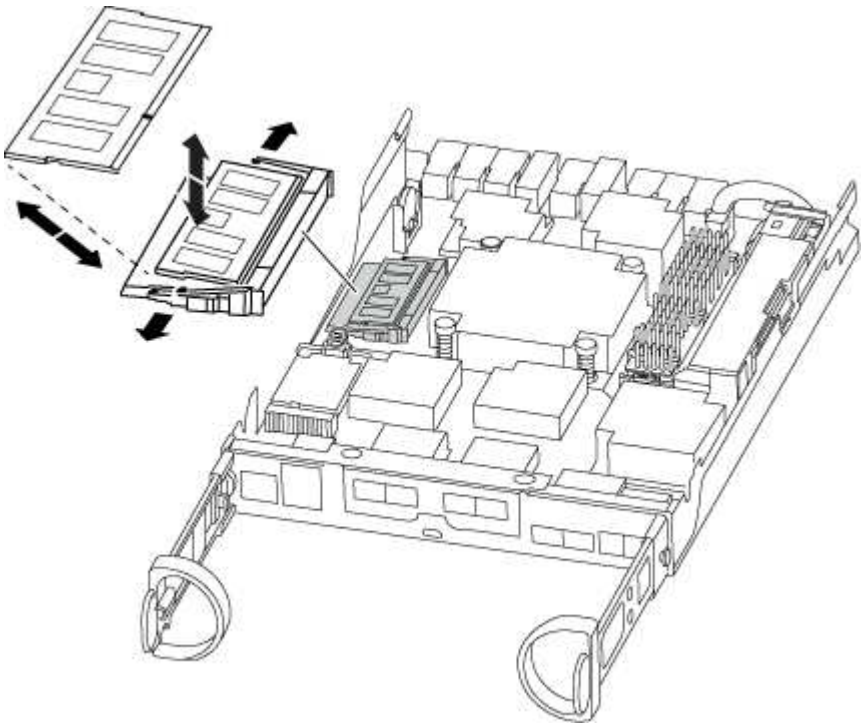
You must have the new controller module ready so that you can move the DIMMs directly from the impaired controller module to the corresponding slots in the replacement controller module.

1. Locate the DIMMs on your controller module.
2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

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

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

   The following illustration shows the location of system DIMMs:



4. Repeat these steps to remove additional DIMMs as needed.
5. Verify that the NVMEM battery is not plugged into the new controller module.
6. Locate the slot where you are installing the DIMM.
7. 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.

8. Repeat these steps for the remaining DIMMs.
9. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

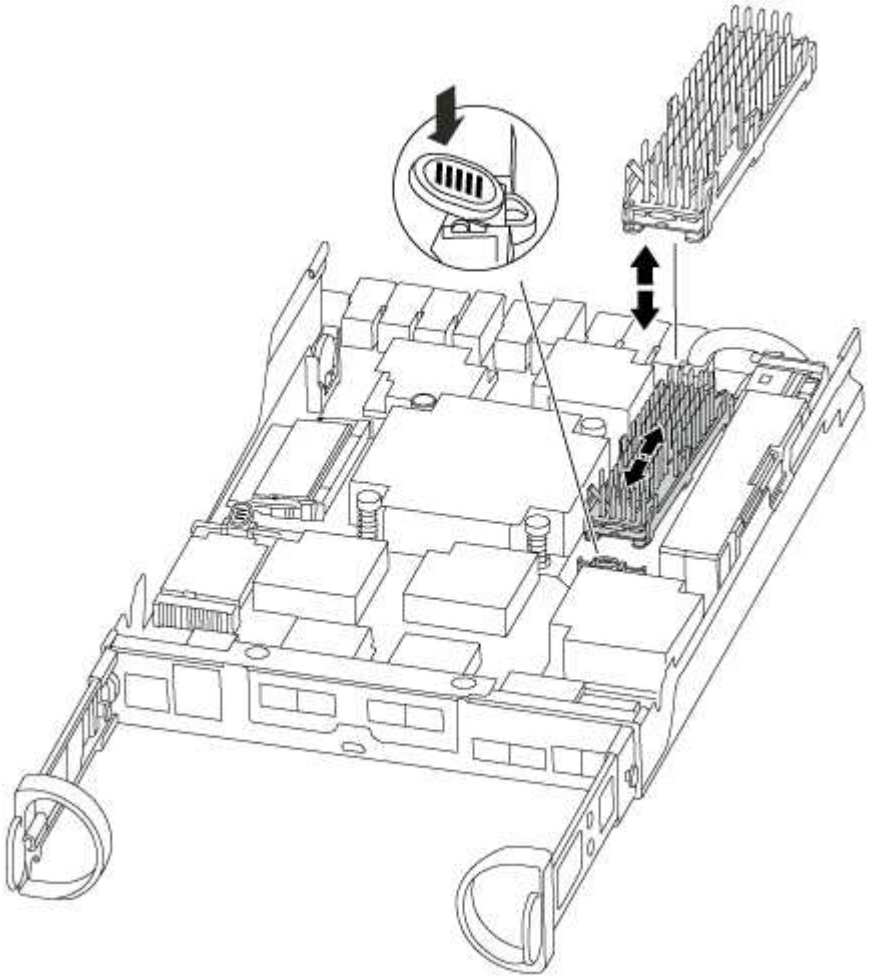
   Make sure that the plug locks down onto the controller module.

### Step 5: Move a caching module, if present

If your AFF A220 or FAS2700 system has a caching module, you need to move the caching module from the old controller module to the replacement controller module. The caching module is referred to as the “M.2 PCIe card” on the controller module label.

You must have the new controller module ready so that you can move the caching module directly from the old controller module to the corresponding slot in the new one. All other components in the storage system must be functioning properly; if not, you must contact technical support.

1. Locate the caching module at the rear of the controller module and remove it.
   a. Press the release tab.
   b. Remove the heatsink.



2. Gently pull the caching module straight out of the housing.
3. Move the caching module to the new controller module, and then align the edges of the caching module with the socket housing and gently push it into the socket.

4. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

5. Reseat and push the heatsink down to engage the locking button on the caching module housing.
6. Close the controller module cover, as needed.

### Step 6: Install the controller

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

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.

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:

| If your system is in… | Then perform these steps… |
| --- | --- |
| An HA pair | The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.<br><br>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.<br><br>ⓘ Do not use excessive force when sliding the controller module into the chassis; you might damage the connectors.<br><br>The controller begins to boot as soon as it is seated in the chassis.<br><br>b. If you have not already done so, reinstall the cable management device.<br><br>c. Bind the cables to the cable management device with the hook and loop strap.<br><br>d. Interrupt the boot process **only** after determining the correct timing:<br><br>You must look for an Automatic firmware update console message. If the update message appears, do not press `Ctrl-C` to interrupt the boot process until after you see a message confirming that the update is complete.<br><br>Only press `Ctrl-C` when you see the message `Press Ctrl-C for Boot Menu`.<br><br>ⓘ If the firmware update is aborted, the boot process exits to the LOADER prompt. You must run the update_flash command and then exit LOADER and boot to Maintenance mode by pressing `Ctrl-C` when you see Starting AUTOBOOT press Ctrl-C to abort.<br><br>If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br><br>e. Select the option to boot to Maintenance mode from the displayed menu. |

| If your system is in… | Then perform these steps… |
| --- | --- |
| A stand-alone configuration | 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.<br><br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br><br>b. If you have not already done so, reinstall the cable management device.<br><br>c. Bind the cables to the cable management device with the hook and loop strap.<br><br>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.<br><br>e. Interrupt the boot process **only** after determining the correct timing:<br><br>You must look for an Automatic firmware update console message. If the update message appears, do not press `Ctrl-C` to interrupt the boot process until after you see a message confirming that the update is complete.<br><br>Only press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message.<br><br>If the firmware update is aborted, the boot process exits to the LOADER prompt. You must run the update_flash command and then exit LOADER and boot to Maintenance mode by pressing `Ctrl-C` when you see Starting AUTOBOOT press Ctrl-C to abort.<br><br>If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br><br>f. From the boot menu, select the option for Maintenance mode. |

**Important:** During the boot process, you might see the following prompts:

- A prompt warning of a system ID mismatch and asking to override the system ID.
- A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
  You can safely respond `y` to these prompts.

# 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 after replacing the controller

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

### About this task

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

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

### Steps

1. 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: `show date`

   The date and time are given in GMT.

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 HA state of the controller module

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

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

**Step 3: Run system-level diagnostics**

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

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

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `halt`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

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

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

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

4. Run diagnostics as desired.

| If you want to run diagnostic tests on… | Then… |
| --- | --- |
| Individual components | a. Clear the status logs: `sldiag device clearstatus`<br>b. Display the available tests for the selected devices: `sldiag device show -dev dev_name`<br><br>*dev_name* can be any one of the ports and devices identified in the preceding step.<br><br>c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only`<br><br>-selection only disables all other tests that you do not want to run for the device.<br><br>d. Run the selected tests: `sldiag device run -dev dev_name`<br><br>After the test is complete, the following message is displayed:<br><br>`*> <SLDIAG:_ALL_TESTS_COMPLETED>`<br><br>e. Verify that no tests failed: `sldiag device status -dev dev_name -long -state failed`<br><br>System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component. |

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

5. Proceed based on the result of the preceding step.

| If the system-level diagnostics tests… | Then… |
| --- | --- |
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>`SLDIAG: No log messages are present.`<br>c. Exit Maintenance mode: `halt`<br>The system displays the LOADER prompt.<br>You have completed system-level diagnostics. |
| Resulted in some test failures | Determine the cause of the problem.<br>a. Exit Maintenance mode: `halt`<br>b. Perform a clean shutdown, and then disconnect the power supplies.<br>c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Reconnect the power supplies, and then power on the storage system.<br>e. Rerun the system-level diagnostics test. |

#### Recable the system and reassign disks - AFF A220 and FAS2700

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

### Step 1: Recable the system

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

**Steps**

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.

c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.

d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

### Step 2: Reassign disks

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

You must use the correct procedure for your configuration:

| Controller redundancy | Then use this procedure… |
|---|---|
| HA pair | Verifying the system ID change on an HA system |
| Stand-alone | Manually reassigning the system ID on a stand-alone system in ONTAP |
| Two-node MetroCluster configuration | Manually reassigning the system ID on systems in a two-node MetroCluster configuration |

### Option 1: Verify the system ID change on an HA system

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

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

1. If the *replacement* controller 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* controller, boot the controller, 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* controller console and then, from the healthy controller, 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 controller, 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`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, 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 controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode` *`replacement_node_name`*

      The *replacement* controller 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 content 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* controller 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 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

#### Option 2: Manually reassign the system ID on a stand-alone system in ONTAP

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

**About this task**

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

**Steps**

1. If you have not already done so, reboot the *replacement* node, interrupt the boot process by pressing Ctrl-C, and then select the option to boot to Maintenance mode from the displayed menu.
2. You must enter `Y` when prompted to override the system ID due to a system ID mismatch.
3. View the system IDs: `disk show -a`
4. You should make a note of the old system ID, which is displayed as part of the disk owner column.

   The following example shows the old system ID of 118073209:

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

  DISK      OWNER                  POOL   SERIAL NUMBER  HOME
--------    -------------          -----  -------------  -------------
disk_name    system-1  (118073209)  Pool0  J8XJE9LC       system-1
(118073209)
disk_name    system-1  (118073209)  Pool0  J8Y478RC       system-1
(118073209)
.
.
.
```

5. Reassign disk ownership by using the system ID information obtained from the disk show command: `disk reassign -s old system ID disk reassign -s 118073209`
6. Verify that the disks were assigned correctly: `disk show -a`

   The disks belonging to the replacement node should show the new system ID. The following example now show the disks owned by system-1 the new system ID, 118065481:

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

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

7. Boot the node: `boot_ontap`

**Option 3: 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) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

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

   You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

   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   system-1  (118065481) Pool0  J8Y0TDZC       system-1
(118065481)
disk_name   system-1  (118065481) Pool0  J8Y09DXC       system-1
(118065481)
.
.
.
```

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

a. Change to the advanced privilege level: `set -privilege advanced`

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

b. Verify that the coredumps are saved: `system node run -node local-node-name partner savecore`

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

c. Return to the admin privilege level: `set -privilege admin`

7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
8. Boot the *replacement* node: `boot_ontap`
9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`
10. Verify the MetroCluster configuration: `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 A220 and FAS2700

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

### Step 1: Install licenses for the replacement controller in ONTAP

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

#### About this task

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

#### Before you begin

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.

#### 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: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption

functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

**Step**

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use 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

### Step 3: Verify LIFs and register the serial number

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

**Steps**

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

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

2. Register the system serial number with NetApp Support.
   - 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. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

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

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

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 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 & Replacements page for further information.

### Replace a DIMM - AFF A220 and FAS2700

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

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

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

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

#### Step 2: Remove controller module

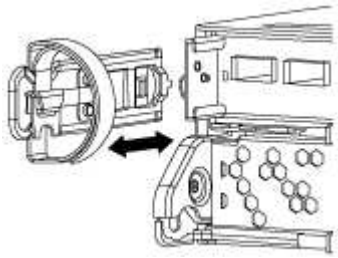
To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

**Steps**

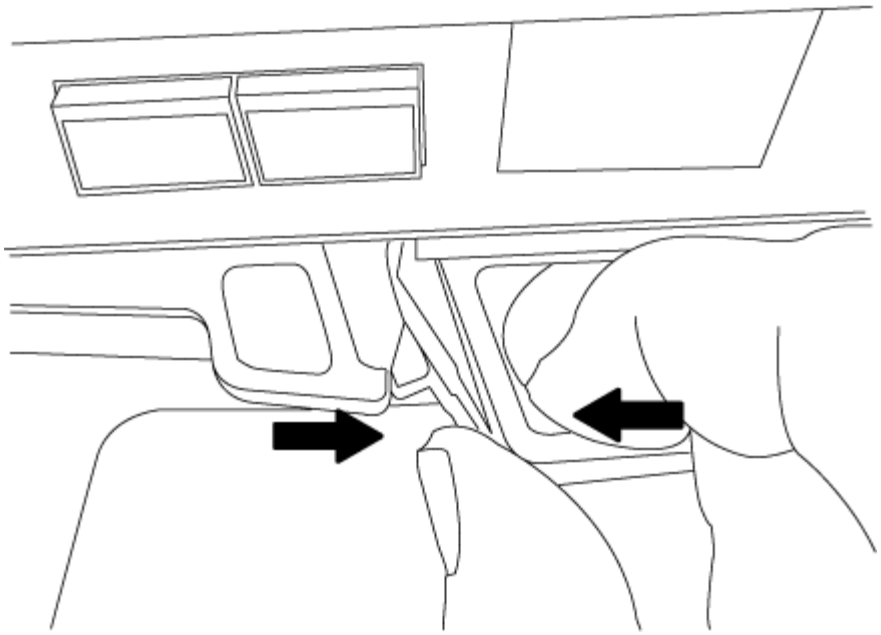
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

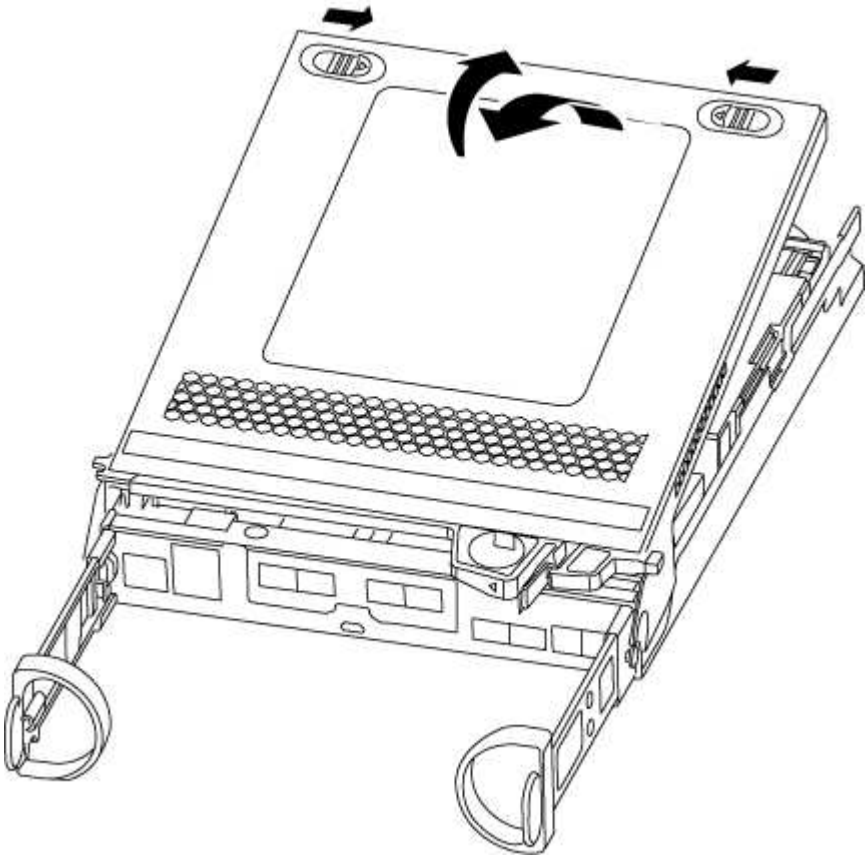
3. Remove and set aside the cable management devices from the left and right sides of the controller module.



4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.



**Step 3: Replace the DIMMs**

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

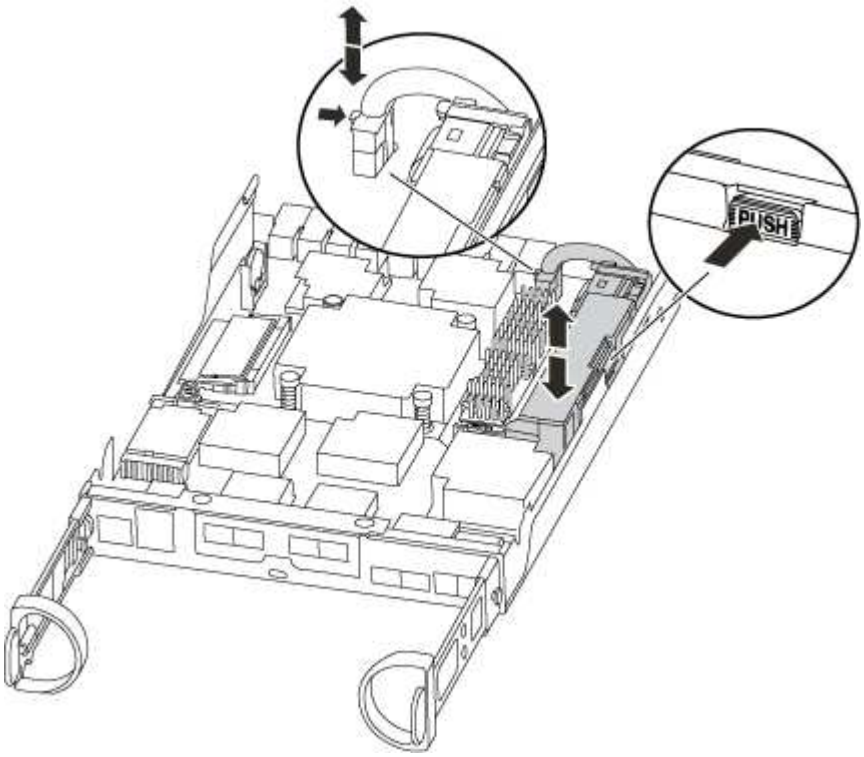
If you are replacing a DIMM, you need to remove it after you have unplugged the NVMEM battery from the controller module.

**Steps**

1. If you are not already grounded, properly ground yourself.
2. Check the NVMEM LED on the controller module.

   You must perform a clean system shutdown before replacing system components to avoid losing unwritten data in the nonvolatile memory (NVMEM). The LED is located on the back of the controller module. Look for the following icon:

3. If the NVMEM LED is not flashing, there is no content in the NVMEM; you can skip the following steps and proceed to the next task in this procedure.
4. If the NVMEM LED is flashing, there is data in the NVMEM and you must disconnect the battery to clear the memory:
   a. Locate the battery, press the clip on the face of the battery plug to release the lock clip from the plug socket, and then unplug the battery cable from the socket.


   b. Confirm that the NVMEM LED is no longer lit.
   c. Reconnect the battery connector.
5. Return to Replace the DIMMs of this procedure to recheck the NVMEM LED.
6. Locate the DIMMs on your controller module.

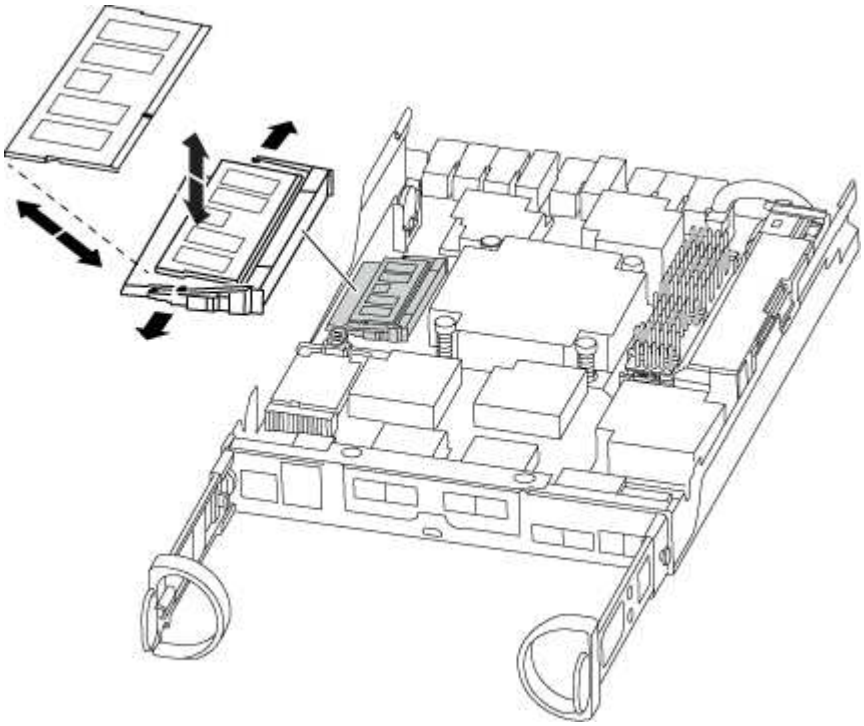
> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.

7. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
8. 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.

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

   The following illustration shows the location of system DIMMs:



9. 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.

10. 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.

11. 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.
12. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

Make sure that the plug locks down onto the controller module.

13. Close the controller module cover.

#### Step 4: Reinstall the controller module

## After you replace components in the controller module, reinstall it into 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. 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.

5. Complete the reinstallation of the controller module:

| If your system is in… | Then perform these steps… |
| --- | --- |
| An HA pair | The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.<br><br>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.<br><br>ⓘ Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br><br>The controller begins to boot as soon as it is seated in the chassis.<br><br>b. If you have not already done so, reinstall the cable management device.<br><br>c. Bind the cables to the cable management device with the hook and loop strap.<br><br>d. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process.<br><br>ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br><br>e. Select the option to boot to Maintenance mode from the displayed menu. |

| If your system is in… | Then perform these steps… |
| --- | --- |
| A stand-alone configuration | 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.<br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. Bind the cables to the cable management device with the hook and loop strap.<br>d. Reconnect the power cables to the power supplies and to the power sources, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message.<br>If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br>e. From the boot menu, select the option for Maintenance mode. |

#### Step 5: Run system-level diagnostics

## After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

**Steps**

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to

function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

| If the system-level diagnostics tests… | Then… |
|---|---|
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>SLDIAG: No log messages are present.<br>c. Exit Maintenance mode: `halt`<br>The controller displays the LOADER prompt.<br>d. Boot the controller from the LOADER prompt: `bye`<br>e. Return the controller to normal operation: |

| If your controller is in… | Then… |
|---|---|
| An HA pair | Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`*<br>If you disabled automatic giveback, re-enable it with the storage failover modify command. |
| A two-node MetroCluster configuration | Proceed to the next step.<br>The MetroCluster switchback procedure is done in the next task in the replacement process. |
| A stand-alone configuration | Proceed to the next step.<br>No action is required.<br>You have completed system-level diagnostics. |

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

#### Step 6: Switch back aggregates in a two-node MetroCluster configuration

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

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 7: 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 & Replacements page for further information.

### Replace SSD Drive or HDD Drive - AFF A220 and FAS2700

You can replace a failed drive nondisruptively while I/O is in progress. The procedure for replacing an SSD is meant for non-spinning drives and the procedure for replacing an HDD is meant for spinning drives.

When a drive fails, the platform logs a warning message to the system console indicating which drive has failed. In addition, both the fault LED on the operator display panel and the fault LED on the failed drive are illuminated.

#### Before you begin

- Follow best practice and install the current version of the Disk Qualification Package (DQP) before replacing a drive.
- Identify the failed disk drive by running the `storage disk show -broken` command from the system console.

  The failed drive appears in the list of failed drives. If it does not, you should wait, and then run the command again.

  > Depending on the drive type and capacity, it can take up to several hours for the drive to appear in the list of failed drives.

- Determine whether SED authentication is enabled.

  How you replace the disk depends on how the disk drive is being used. If SED authentication is enabled, you must use the SED replacement instructions in the ONTAP 9 NetApp Encryption Power Guide. These Instructions describe additional steps you must perform before and after replacing an SED.

- Make sure the replacement drive is supported by your platform. See the NetApp Hardware Universe.
- Make sure all other components in the system are functioning properly; if not, you must contact technical support.

#### About this task

Drive firmware is automatically updated (nondisruptively) on new drives that have non current firmware versions.

When replacing several disk drives, you must wait one minute between the removal of each failed disk drive and the insertion of the replacement disk drive to allow the storage system to recognize the existence of each new disk.

#### Procedure

Replace the failed drive by selecting the option appropriate to the drives that your platform supports.

You may also choose to watch the Replace failed drive video that shows an overview of the embedded drive replacement procedure.

**Option 1: Replace SSD**

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Physically identify the failed drive.

   When a drive fails, the system logs a warning message to the system console indicating which drive failed. Additionally, the attention (amber) LED on the drive shelf operator display panel and the failed drive illuminate.

   > The activity (green) LED on a failed drive can be illuminated (solid), which indicates that the drive has power, but should not be blinking, which indicates I/O activity. A failed drive has no I/O activity.

4. Remove the failed drive:
   a. Press the release button on the drive face to open the cam handle.
   b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.
5. Wait a minimum of 70 seconds before inserting the replacement drive.

   This allows the system to recognize that a drive was removed.

6. Insert the replacement drive:
   a. With the cam handle in the open position, use both hands to insert the replacement drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

7. Verify that the drive’s activity (green) LED is illuminated.

   When the drive’s activity LED is solid, it means that the drive has power. When the drive’s activity LED

is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

8. If you are replacing another drive, repeat Steps 3 through 7.
9. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
   a. Display all unowned drives: `storage disk show -container-type unassigned`

      You can enter the command on either controller module.

   b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

      You can enter the command on either controller module.

      You can use the wildcard character to assign more than one drive at once.

   c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

      You must reenable automatic drive assignment on both controller modules.

10. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

**Option 2: Replace HDD**

1. If you want to manually assign drive ownership for the replacement drive, you need to disable automatic drive assignment replacement drive, if it is enabled

   > You manually assign drive ownership and then reenable automatic drive assignment later in this procedure.

   a. Verify whether automatic drive assignment is enabled: `storage disk option show`

      You can enter the command on either controller module.

      If automatic drive assignment is enabled, the output shows `on` in the “Auto Assign” column (for each controller module).

   b. If automatic drive assignment is enabled, disable it: `storage disk option modify -node node_name -autoassign off`

      You must disable automatic drive assignment on both controller modules.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the failed disk drive from the system console warning message and the illuminated fault LED on the disk drive
5. Press the release button on the disk drive face.

Depending on the storage system, the disk drives have the release button located at the top or on the left of the disk drive face.

For example, the following illustration shows a disk drive with the release button located on the top of the disk drive face:

The cam handle on the disk drive springs open partially and the disk drive releases from the midplane.

6. Pull the cam handle to its fully open position to unseat the disk drive from the midplane.

7. Slide out the disk drive slightly and allow the disk to safely spin down, which can take less than one minute, and then, using both hands, remove the disk drive from the disk shelf.
8. With the cam handle in the open position, insert the replacement disk drive into the drive bay, firmly pushing until the disk drive stops.

   Wait a minimum of 10 seconds before inserting a new disk drive. This allows the system to recognize that a disk drive was removed.

   If your platform drive bays are not fully loaded with drives, it is important to place the replacement drive into the same drive bay from which you removed the failed drive.

   Use two hands when inserting the disk drive, but do not place hands on the disk drive boards that are exposed on the underside of the disk carrier.

9. Close the cam handle so that the disk drive is fully seated into the midplane and the handle clicks into place.

   Be sure to close the cam handle slowly so that it aligns correctly with the face of the disk drive..

10. If you are replacing another disk drive, repeat Steps 4 through 9.
11. Reinstall the bezel.
12. If you disabled automatice drive assignment in Step 1, then, manually assign drive ownership and then reenable automatic drive assignment if needed.
    a. Display all unowned drives: `storage disk show -container-type unassigned`

       You can enter the command on either controller module.

    b. Assign each drive: `storage disk assign -disk disk_name -owner owner_name`

       You can enter the command on either controller module.

       You can use the wildcard character to assign more than one drive at once.

    c. Reenable automatic drive assignment if needed: `storage disk option modify -node node_name -autoassign on`

       You must reenable automatic drive assignment on both controller modules.

13. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

### Replace the NVMEM battery - AFF A220 and FAS2700

To replace an NVMEM battery in the system, you must remove the controller module from the system, open it, replace the battery, and close and replace the controller module.

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

#### Step 1: Shut down the impaired controller

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

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

#### Step 2: Remove controller module

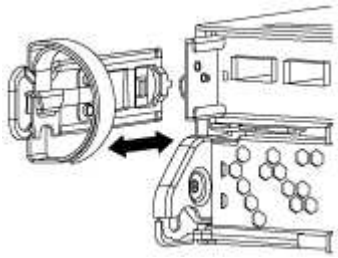
To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

**Steps**

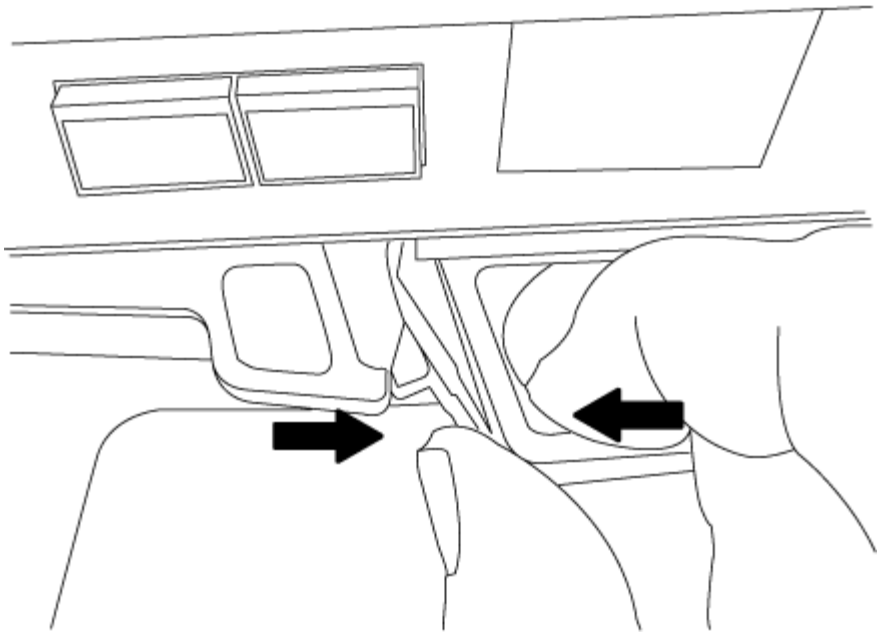
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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



4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.

#### Step 3: Replace the NVMEM battery

To replace the NVMEM battery in your system, you must remove the failed NVMEM battery from the system and replace it with a new NVMEM battery.

**Steps**

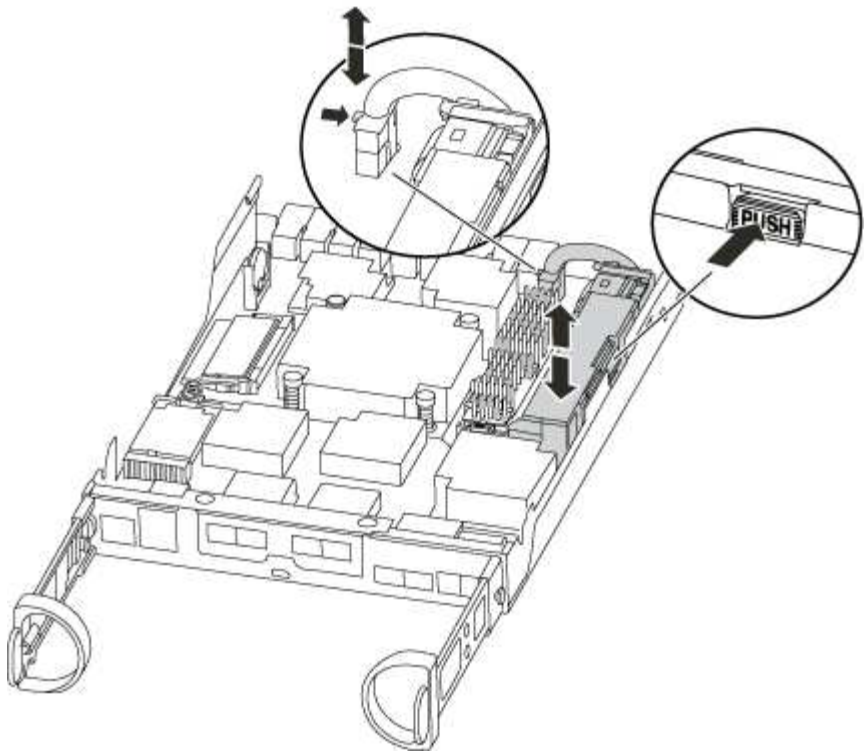
1. If you are not already grounded, properly ground yourself.
2. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

3. Locate the NVMEM battery in the controller module.




4. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
5. Remove the battery from the controller module and set it aside.
6. Remove the replacement battery from its package.
7. Loop the battery cable around the cable channel on the side of the battery holder.
8. Position the battery pack by aligning the battery holder key ribs to the “V” notches on the sheet metal side wall.
9. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots on the battery pack, and the battery pack latch engages and clicks into the opening on the side wall.
10. Plug the battery plug back into the controller module.

#### Step 4: Reinstall the controller module

## After you replace components in the controller module, reinstall it into 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. 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.

5. Complete the reinstallation of the controller module:

| If your system is in… | Then perform these steps… |
|---|---|
| An HA pair | The controller module begins to boot as soon as it is fully seated in the chassis. Be prepared to interrupt the boot process.<br><br>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.<br><br>ⓘ Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br><br>The controller begins to boot as soon as it is seated in the chassis.<br><br>b. If you have not already done so, reinstall the cable management device.<br><br>c. Bind the cables to the cable management device with the hook and loop strap.<br><br>d. When you see the message `Press Ctrl-C for Boot Menu`, press `Ctrl-C` to interrupt the boot process.<br><br>ⓘ If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br><br>e. Select the option to boot to Maintenance mode from the displayed menu. |

| If your system is in… | Then perform these steps… |
| --- | --- |
| A stand-alone configuration | 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.<br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. Bind the cables to the cable management device with the hook and loop strap.<br>d. Reconnect the power cables to the power supplies and to the power sources, turn on the power to start the boot process, and then press `Ctrl-C` after you see the `Press Ctrl-C for Boot Menu` message.<br>If you miss the prompt and the controller module boots to ONTAP, enter `halt`, and then at the LOADER prompt enter `boot_ontap`, press `Ctrl-C` when prompted, and then boot to Maintenance mode.<br>e. From the boot menu, select the option for Maintenance mode. |

#### Step 5: Run system-level diagnostics

## After installing a new NVMEM battery, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

**Steps**

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to

function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the NVMEM memory: `sldiag device run -dev nvmem`
4. Verify that no hardware problems resulted from the replacement of the NVMEM battery: `sldiag device status -dev nvmem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

| If the system-level diagnostics tests… | Then… |
|---|---|
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>SLDIAG: No log messages are present.<br>c. Exit Maintenance mode: `halt`<br>The controller displays the LOADER prompt.<br>d. Boot the controller from the LOADER prompt: `bye`<br>e. Return the controller to normal operation: |

| If your controller is in… | Then… |
|---|---|
| An HA pair | Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`*<br>If you disabled automatic giveback, re-enable it with the storage failover modify command. |
| A two-node MetroCluster configuration | Proceed to the next step.<br>The MetroCluster switchback procedure is done in the next task in the replacement process. |
| A stand-alone configuration | Proceed to the next step.<br>No action is required.<br>You have completed system-level diagnostics. |

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

#### Step 6: Switch back aggregates in a two-node MetroCluster configuration

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

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 7: 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 & Replacements page for further information.

### Swap out a power supply - AFF A220 and FAS2700

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.

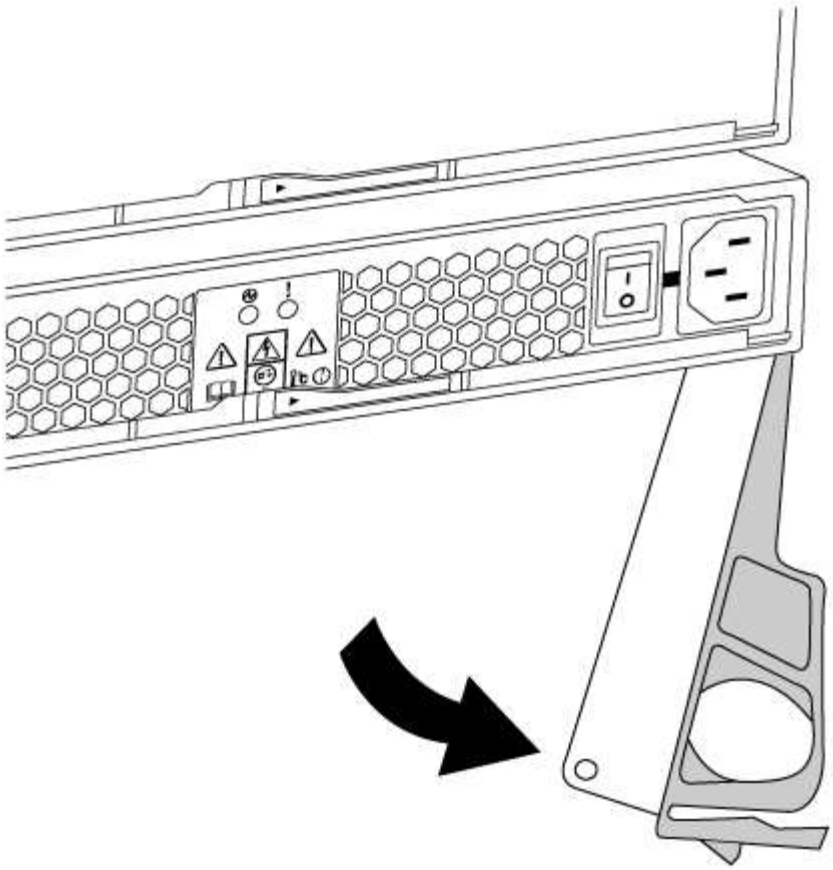
- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> Cooling is integrated with the power supply, so you must replace the power supply within two minutes of removal to prevent overheating due to reduced airflow. Because the chassis provides a shared cooling configuration for the two HA nodes, a delay longer than two minutes will shut down all controller modules in the chassis. If both controller modules do shut down, make sure that both power supplies are inserted, turn both off for 30 seconds, and then turn both on.

- Power supplies are auto-ranging.

**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. Squeeze the latch on the power supply cam handle, and then open the cam handle to fully release the power supply from the mid plane.



5. Use the cam handle to slide the power supply out of the system.

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

6. Make sure that the on/off switch of the new power supply is in the Off position.
7. 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 using the cam handle.

   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.

8. Close the cam handle so that the latch clicks into the locked position and the power supply is fully seated.
9. 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.

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

    The power supply LEDs are lit when the power supply comes online.

11. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Replace the real-time clock battery

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.

#### Step 1: Shut down the impaired controller

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

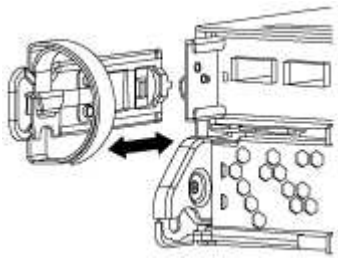
**Step 2: Remove controller module**

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.

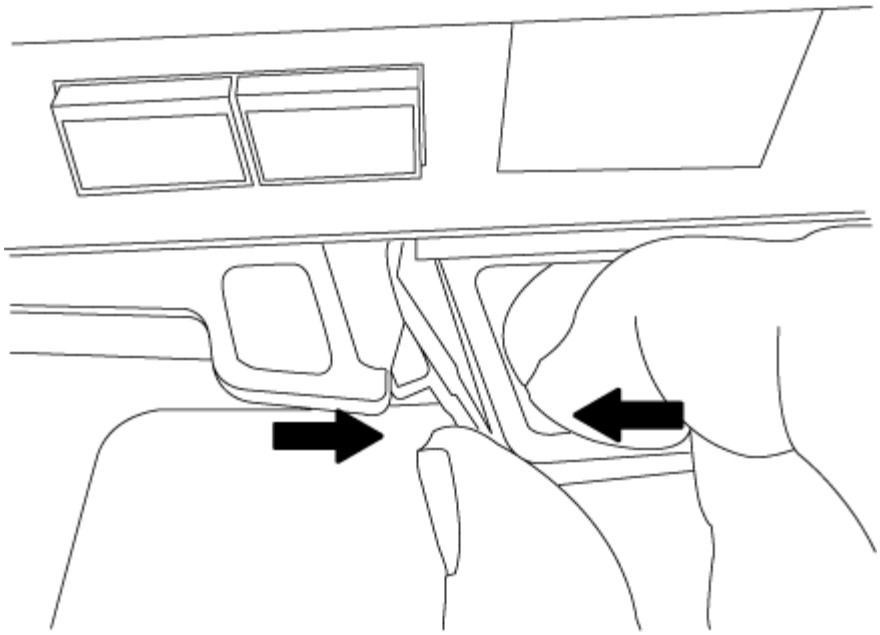
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

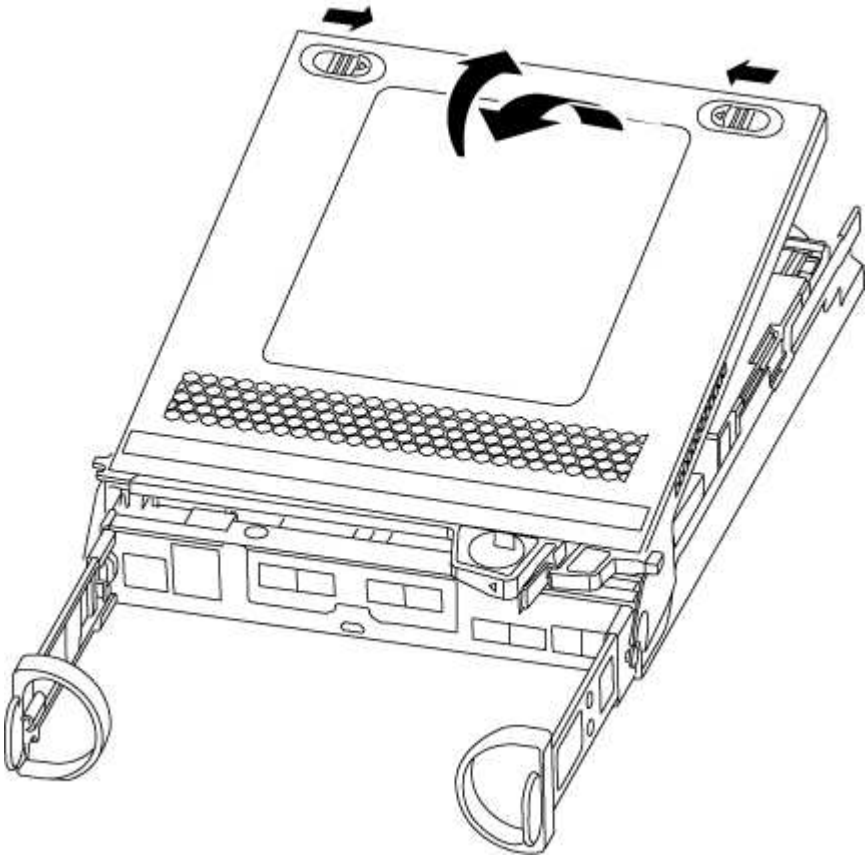
3. Remove and set aside the cable management devices from the left and right sides of the controller module.



4. Squeeze the latch on the cam handle until it releases, open the cam handle fully to release the controller module from the midplane, and then, using two hands, pull the controller module out of the chassis.



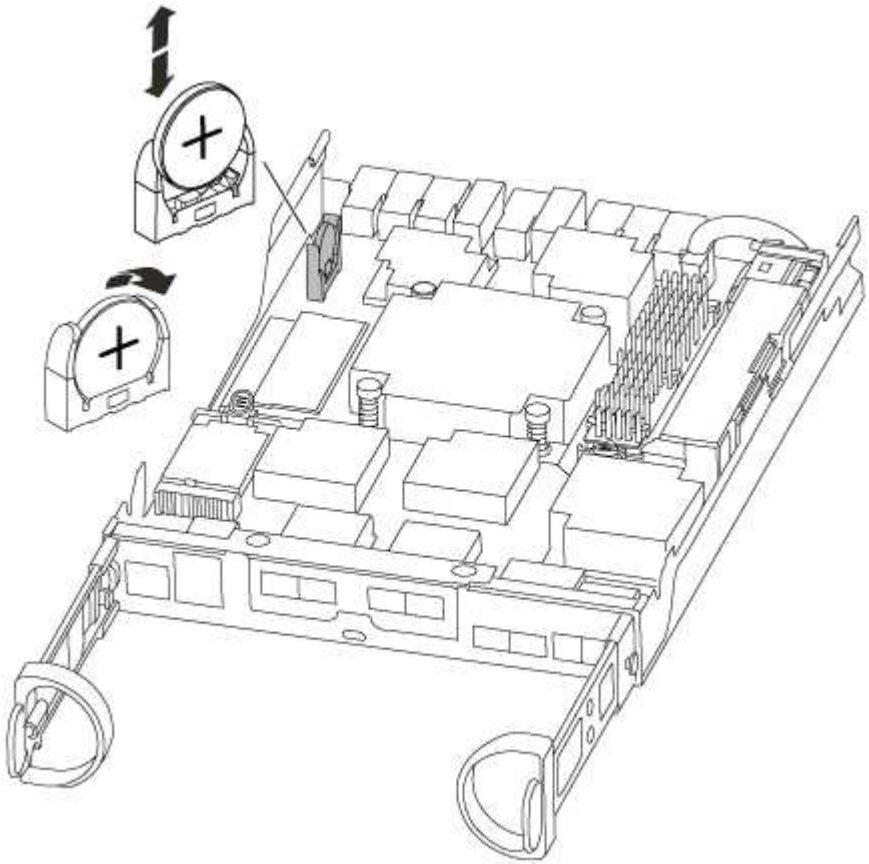
5. Turn the controller module over and place it on a flat, stable surface.
6. Open the cover by sliding in the blue tabs to release the cover, and then swing the cover up and open.



**Step 3: Replace the RTC battery**

To replace the RTC battery, locate it inside the controller and follow the specific sequence of steps.

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



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.

#### Step 4: Reinstall the controller module and set time/date after RTC battery replacement

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.

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 controller with the `show date` command.
   b. At the LOADER prompt on the target controller, 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 controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller 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

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

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 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 & Replacements page for further information.

# FAS8200 System Documentation

## Install and setup

### Cluster configuration worksheet - FAS8200

You can use the Cluster Configuration Worksheet to gather and record your site-specific IP addresses and other information required when configuring an ONTAP cluster.

### Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

For MetroCluster configurations, see either:

- Install MetroCluster IP configuration
- Install MetroCluster Fabric-Attached configuration

### Installation and setup PDF poster - FAS8200

You can use the PDF poster to install and set up your new system. The AFF FAS8200 Installation and Setup Instructions provides step-by-step instructions with live links to additional content.

### Installation and setup video - FAS8200

The following video shows end-to-end software configuration for systems running ONTAP 9.2.

AFF FAS8200 Setup Video

## Maintain

### Boot media

#### Overview of boot media replacement - FAS8200

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` file.

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 must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

#### Check onboard encryption - FAS8200

## Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check what version of ONTAP the system is running.

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

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 the NetApp Encryption overview with the CLI.

**Steps**

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. 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`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support

NVE, proceed to shut down the controller.

- If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to [Option 1: Checking NVE or NSE on systems running ONTAP 9.5 and earlier].
- If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to [Option 2: Checking NVE or NSE on systems running ONTAP 9.6 and later].

4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

### Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

#### Steps

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

### Verify NVE configuration

#### Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps.
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes` manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shutdown the controller.

### Verify NSE configuration

#### Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`

   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps

2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:

   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager`

```
restore -address *
```

If the command fails, contact NetApp Support.

mysupport.netapp.com

b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to back up the OKM information: `security key-manager backup show`

        Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

      - Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shut down the controller.

**Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later**

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

**Verify NVE configuration**

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`
     e. Shut down the impaired controller.
  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
     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.

        mysupport.netapp.com

b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

> Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

### Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:

a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

b. Enter the command to display the key management information: `security key-manager`

`onboard show-backup`

c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

d. Return to admin mode: `set -priv admin`

e. You can safely shut down the controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

   c. You can safely shut down the controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

#### Shut down the impaired controller - FAS8200

**Option 1: Most systems**

After completing the NVE or NSE tasks, you need to complete the shutdown of the impaired controller.
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 `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name`<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

1. 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 configuration**

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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### Option 3: 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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

#### Replace the boot media - FAS8200

## 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.

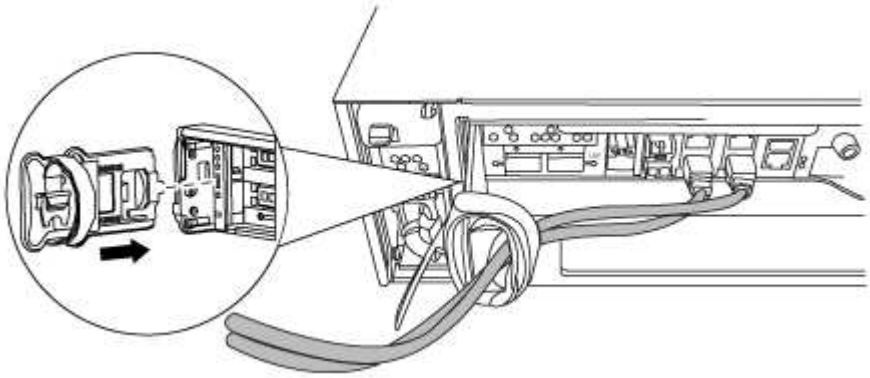
### Step 1: Remove the controller

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.

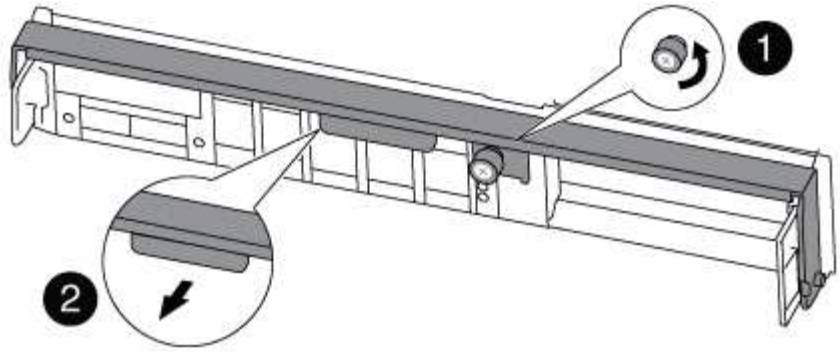
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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



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



| | |
|---|---|
| 1 | |
| Thumbscrew | |
| 2 | |
| Cam handle | |

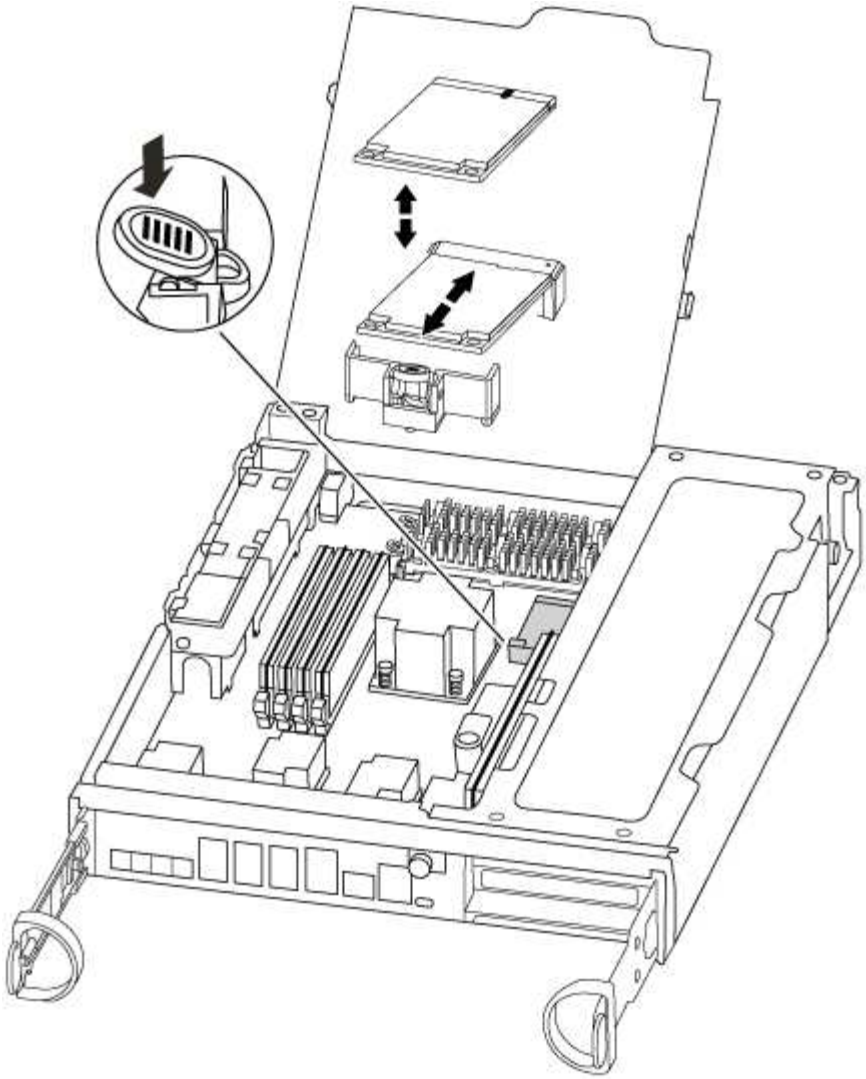
5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

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

**Step 2: Replace the boot media**

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

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



3. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

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

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

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

6. Push the boot media down to engage the locking button on the boot media housing.
7. Close the controller module cover.

### 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 an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs) if they were removed.

3. Insert the USB flash drive into the USB slot on the controller module.

   Make sure that you install the USB flash drive in the slot labeled for USB devices, and not in the USB console port.

4. Push the controller module all the way into the system, making sure that the cam handle clears the USB flash drive, firmly push the cam handle to finish seating the controller module, push the cam handle to the closed position, and then tighten the thumbscrew.

   The controller 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 controller to boot to LOADER.

6. For systems with one controller in the chassis, reconnect the power and turn on the power supplies.

   The system begins to boot and stops at the LOADER prompt.

7. 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 controller from the healthy controller 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.

8. 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 - FAS8200

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

### Option 1: 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 | a. Press `y` when prompted to restore the backup configuration.<br>b. Set the healthy controller to advanced privilege level: `set -privilege advanced`<br>c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`*<br>d. Return the controller to admin level: `set -privilege admin`<br>e. Press `y` when prompted to use the restored configuration.<br>f. Press `y` when prompted to reboot the controller. |
| No network connection | a. Press `n` when prompted to restore the backup configuration.<br>b. Reboot the system when prompted by the system.<br>c. Select the **Update flash from backup config** (sync flash) option from the displayed menu.<br><br>If you are prompted to continue with the update, press `y`. |

4. Ensure that the environmental variables are set as expected:
   a. Take the controller 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 controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

7. Connect the console cable to the partner controller.

8. Give back the controller 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 controller 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: Controller is in a two-node MetroCluster**

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 - FAS8200

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

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 OKM, NSE, and NVE as needed - FAS8200

## Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

### Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

#### Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
|---|---|
| The LOADER prompt | Boot the controller to the boot menu: `boot_ontap menu` |
| Waiting for giveback… | a. Enter `Ctrl-C` at the prompt<br>b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y`<br>c. At the LOADER prompt, enter the `boot_ontap menu` command. |

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

> The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

Example of backup data:


```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.
9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      > Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.
    b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
14. If you are running ONTAP 9.6 or later:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

### Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

**Steps**

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
| --- | --- |
| The login prompt | Go to Step 7. |
| Waiting for giveback… | a. Log into the partner controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.
12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

### Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

#### Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
|---|---|
| The login prompt | Go to Step 7. |
| Waiting for giveback… | a. Log into the partner controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.
   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.

- If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.

5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

    - If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

      Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

#### Return the failed part to NetApp - FAS8200

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Replace the caching module - FAS8200

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation.

You might want to erase the contents of your caching module before replacing it.

. Although data on the caching module is encrypted, you might want to erase any data from the impaired caching module and verify that the caching module has no data:
.. Erase the data on the caching module: `system controller flash-cache secure-erase run`
.. Verify that the data has been erased from the caching module: `system controller flash-cache secure-erase show -node node_name`

+
The output should display the caching module status as erased.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

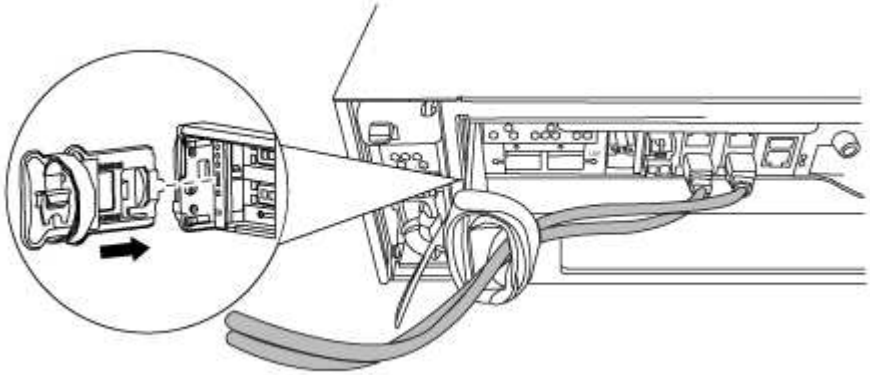
**Step 2: Open the controller module**

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.

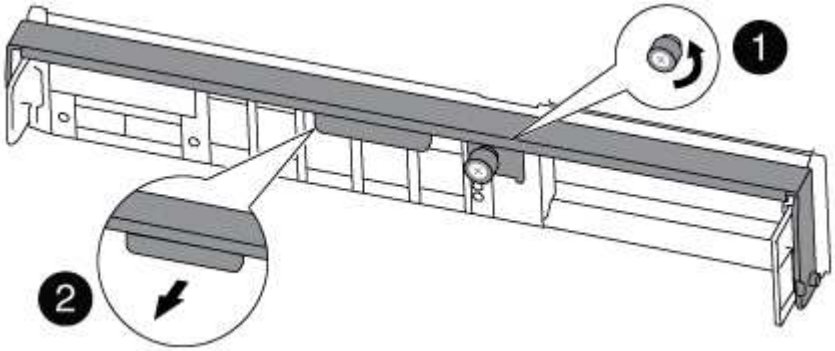
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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



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




| | |
|---|---|
| 1 | Thumbscrew |
| 2 | Cam handle |

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

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

#### Step 3: Replace or add a caching module

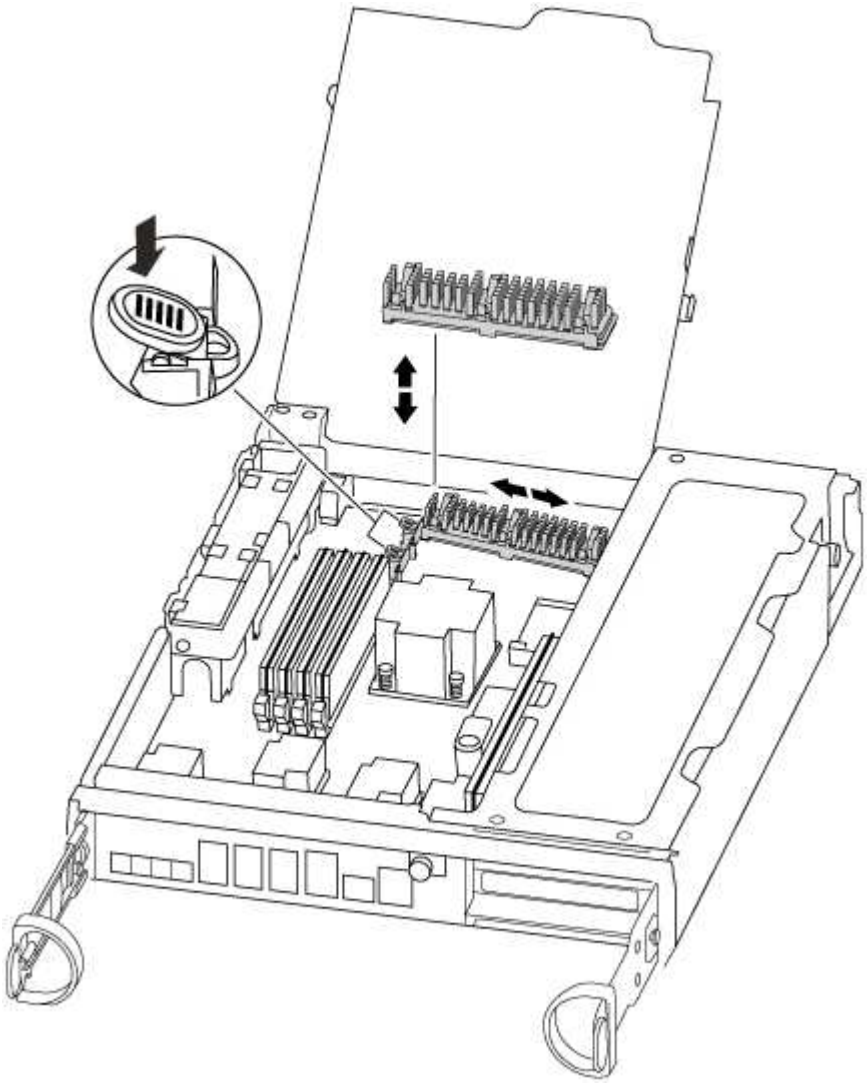
To replace or add a caching module referred to as the M.2 PCIe card on the label on your controller, locate the slots inside the controller and follow the specific sequence of steps.

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

1. Locate the caching module at the rear of the controller module and remove it.
   a. Press the release tab.
   b. Remove the heatsink.

      The storage system comes with two slots available for the caching module and only one slot is occupied, by default.



2. If you are adding a caching module, go to the next step; if you are replacing the caching module, gently pull it straight out of the housing.

3. Align the edges of the caching module with the socket in the housing, and then gently push it into the socket.
4. Verify that the caching module is seated squarely and completely in the socket.

   If necessary, remove the caching module and reseat it into the socket.

5. Reseat and push the heatsink down to engage the locking button on the caching module housing.
6. Repeat the steps if you have a second caching module. Close the controller module cover, as needed.

#### Step 4: Reinstall the controller

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it to a state where you can run diagnostic tests on the replaced component.

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 system, as needed.

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

3. Complete the reinstallation of the controller module:

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

   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

   b. Tighten the thumbscrew on the cam handle on back of the controller module.
   c. If you have not already done so, reinstall the cable management device.
   d. Bind the cables to the cable management device with the hook and loop strap.
   e. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.
   f. Select the option to boot to Maintenance mode from the displayed menu.

#### Step 5: Run system-level diagnostics

After installing a new caching module, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the caching module: `sldiag device run -dev fcache`
4. Verify that no hardware problems resulted from the replacement of the caching module: `sldiag device status -dev fcache -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

| If the system-level diagnostics tests… | Then… |
|---|---|
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>SLDIAG: No log messages are present.<br>c. Exit Maintenance mode: `halt`<br>The controller displays the LOADER prompt.<br>d. Boot the controller from the LOADER prompt: `bye`<br>e. Return the controller to normal operation: |

| If your controller is in… | Then… |
|---|---|
| An HA pair | Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`*<br>If you disabled automatic giveback, re-enable it with the storage failover modify command. |

| If your controller is in… | Then… |
| --- | --- |
| A two-node MetroCluster configuration | Proceed to the next step.<br>The MetroCluster switchback procedure is done in the next task in the replacement process. |
| A stand-alone configuration | Proceed to the next step. No action is required. You have completed system-level diagnostics. |
| Resulted in some test failures | Determine the cause of the problem:<br>a. Exit Maintenance mode: `halt`<br>After you issue the command, wait until the system stops at the LOADER prompt.<br>b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis:<br>◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module.<br>◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources.<br>c. Verify that you have observed all the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu:<br>◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis.<br>The controller module boots up when fully seated.<br>◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on.<br>e. Select Boot to maintenance mode from the menu.<br>f. Exit Maintenance mode by entering the following command: `halt`<br>After you issue the command, wait until the system stops at the LOADER prompt.<br>g. Rerun the system-level diagnostic test. |

#### Step 6: Switch back aggregates in a two-node MetroCluster configuration

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

local disk pools.

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 7: Complete the replacement process

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Chassis

#### Overview of chassis replacement - FAS8200

To replace the chassis, you must move the power supplies, fans, and controller 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.

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 written with the assumption that you are moving the controller module or modules to the new chassis, and that the chassis is a new component from NetApp.
- This procedure is disruptive. For a two-controller cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

#### Shut down the controllers - FAS8200

To replace the chassis, you must shutdown the controllers.

### Option 1: Most configurations

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

#### About this task

- If you have a cluster with more than two controllers, 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 the Administration overview with the CLI.
- 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`

#### Steps

1. If your system has two controller modules, disable the HA pair.

| If your system is running clustered ONTAP with… | Then… |
| --- | --- |
| Two controllers in the cluster | `cluster ha modify -configured false` `storage failover modify -node node0 -enabled false` |
| More than two controllers in the cluster | `storage failover modify -node node0 -enabled false` |

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

### Option 2: Controller is 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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

#### Replace hardware - FAS8200

## Move the power supplies, fans, and controller 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: Move a power supply

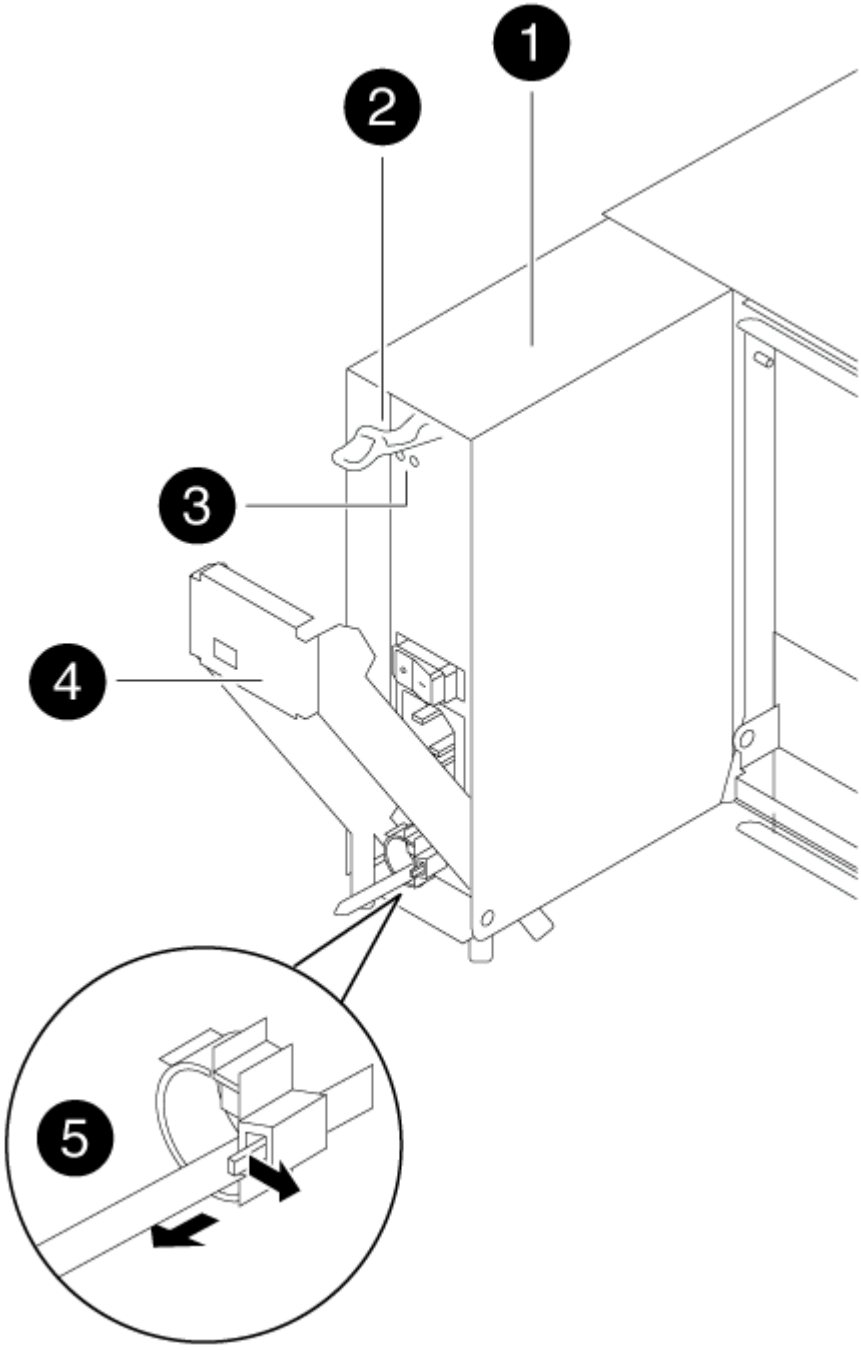
Moving out a power supply when replacing a chassis involves turning off, disconnecting, and removing the power supply from the old chassis and installing and connecting it on the replacement chassis.

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 down the release latch on the power supply cam handle, and then lower the cam handle to the fully open position to release the power supply from the mid plane.




| | |
|---|---|
| 1 | Power supply |
| 2 | Cam handle release latch |

| | |
|---|---|
| 3 | Power and Fault LEDs |
| 4 | Cam handle |
| 5 | Power cable locking mechanism |

4. Use the cam handle to slide the power supply out of the system.

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

5. Repeat the preceding steps for any remaining power supplies.
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 using the cam handle.

   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. Push firmly on the power supply cam handle to seat it all the way into the chassis, and then push the cam handle to the closed position, making sure that the cam handle release latch clicks into its locked position.
8. Reconnect the power cable and secure it to the power supply using the power cable locking mechanism.

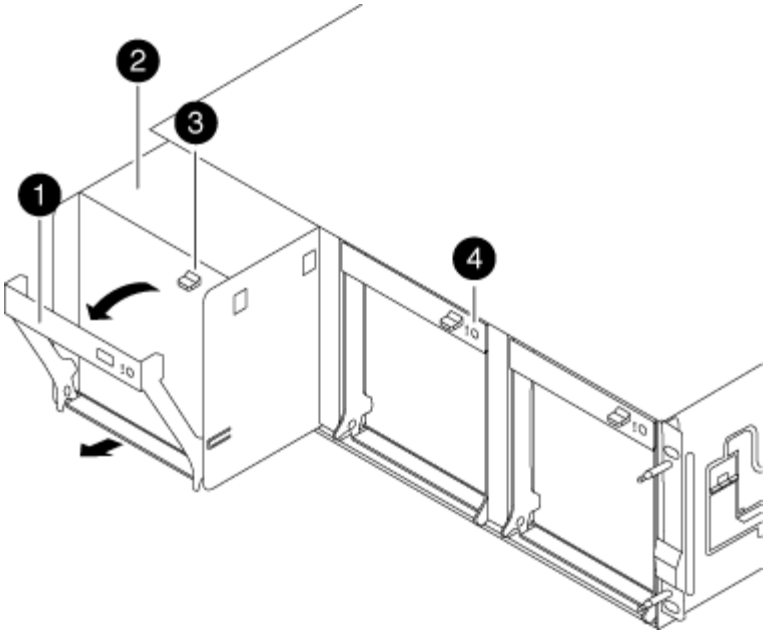
   Only connect the power cable to the power supply. Do not connect the power cable to a power source at this time.

**Step 2: Move a fan**

Moving out a fan module when replacing the chassis involves a specific sequence of tasks.

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 down the release latch on the fan module cam handle, and then pull the cam handle downward.

   The fan module moves a little bit away from the chassis.



| | |
|---|---|
| 1 | Cam handle |
| 2 | Fan module |
| 3 | Cam handle release latch |
| 4 | Fan module Attention LED |

3. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

   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.

4. Set the fan module aside.
5. Repeat the preceding steps for any remaining fan modules.
6. Insert the fan module into the replacement chassis by aligning it with the opening, and then sliding it into the chassis.
7. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

8. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The fan LED should be green after the fan is seated and has spun up to operational speed.

9. Repeat these steps for the remaining fan modules.

10. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.

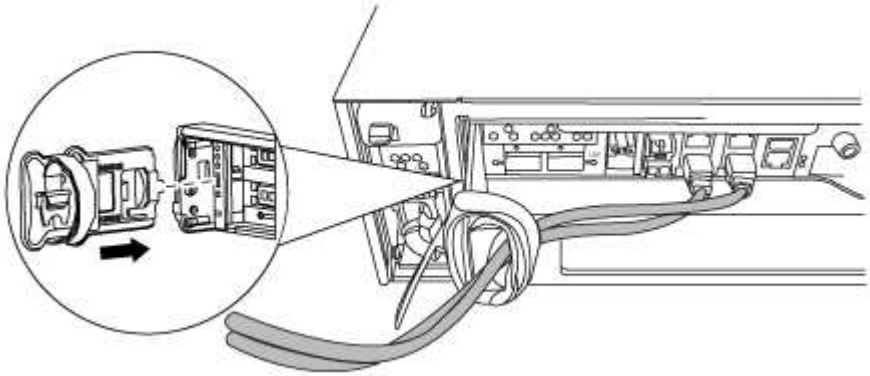
**Step 3: Remove the controller module**

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

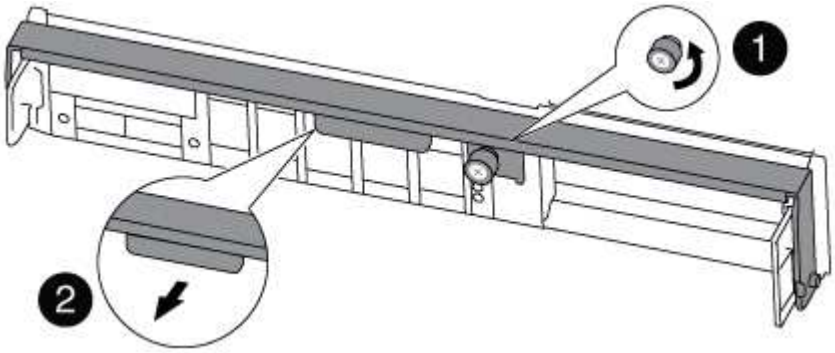
1. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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



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




| | |
|---|---|
| 1 | Thumbscrew |
| 2 | Cam handle |

4. Pull the cam handle downward and begin to slide the controller module out of the chassis.

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

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

### Step 4: Replace a chassis from within the equipment rack or system cabinet

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. If you have not already done so, install the bezel.

### Step 5: Install the controller

After you install the controller module and any other components into the new chassis, boot it to a state where you can run the interconnect diagnostic test.

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.

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. Repeat the preceding steps if there is a second controller to install in the new chassis.
4. Complete the installation of the controller module:

| If your system is in… | Then perform these steps… |
| --- | --- |
| An HA pair | a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module.<br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. Bind the cables to the cable management device with the hook and loop strap.<br>d. Repeat the preceding steps for the second controller module in the new chassis. |
| A stand-alone configuration | a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module.<br>Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. Bind the cables to the cable management device with the hook and loop strap.<br>d. Reinstall the blanking panel and then go to the next step. |

5. Connect the power supplies to different power sources, and then turn them on.
6. Boot each controller to Maintenance mode:
   a. As each controller 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.

#### Restore and verify the configuration - FAS8200

You must verify the HA state of the chassis and run System-Level diagnostics, switch back aggregates, 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.

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. The next step depends on your system configuration.

| If your system is in… | Then… |
|---|---|
| A stand-alone configuration | a. Exit Maintenance mode: `halt`<br>b. Go to "Completing the replacement process. |
| An HA pair with a second controller module | Exit Maintenance mode: `halt` The LOADER prompt appears. |

### Step 2: Run system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

> During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second controller if you are in an HA configuration.

   > Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

| If the system-level diagnostics tests… | Then… |
| --- | --- |
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>`SLDIAG: No log messages are present.`<br>c. Exit Maintenance mode on both controllers: `halt`<br>The system displays the LOADER prompt.<br>You must exit Maintenance mode on both controllers before proceeding any further.<br>d. Enter the following command on both controllers at the LOADER prompt: `bye`<br>e. Return the controller to normal operation: |

| If your system is running ONTAP… | Then… |
| --- | --- |
| With two nodes in the cluster | Issue these commands: `node::> cluster ha modify -configured true``node::> storage failover modify -node node0 -enabled true` |
| With more than two nodes in the cluster | Issue this command:`node::> storage failover modify -node node0 -enabled true` |
| In a two-node MetroCluster configuration | Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process. |
| In a stand-alone configuration | You have no further steps in this particular task.<br>You have completed system-level diagnostics. |

| If your system is running ONTAP… | Then… |
| --- | --- |
| Resulted in some test failures | Determine the cause of the problem.<br>a. Exit Maintenance mode: `halt`<br>b. Perform a clean shutdown, and then disconnect the power supplies.<br>c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Reconnect the power supplies, and then power on the storage system.<br>e. Rerun the system-level diagnostics test. |

### Step 3: Switch back aggregates in a two-node MetroCluster configuration

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

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 & Replacements page for further information.

### Controller

#### Overiew of controller module replacement - FAS8200

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 is a FlexArray system or 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 controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- 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 controller in a four or eight controller 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.

- This procedure includes steps for automatically or manually reassigning drives to the *replacement* controller, depending on your system's configuration.

  You should perform the drive reassignment as directed in the procedure.

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the *replacement* controller so that the *replacement* controller will boot up in the same version of ONTAP as the old controller module.
- Any PCIe cards moved from the old controller module to the new controller module or added from existing customer site inventory must be supported by the replacement controller module.

  NetApp Hardware Universe

- It is important that you apply the commands in these steps on the correct systems:
  - The *impaired* controller is the controller that is being replaced.
  - The *replacement* controller is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller'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 - FAS8200

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware 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 are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the “Returning SEDs to unprotected mode” section of the *ONTAP 9 NetApp Encryption Power Guide*.

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

#### Replace the controller module hardware - FAS8200

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

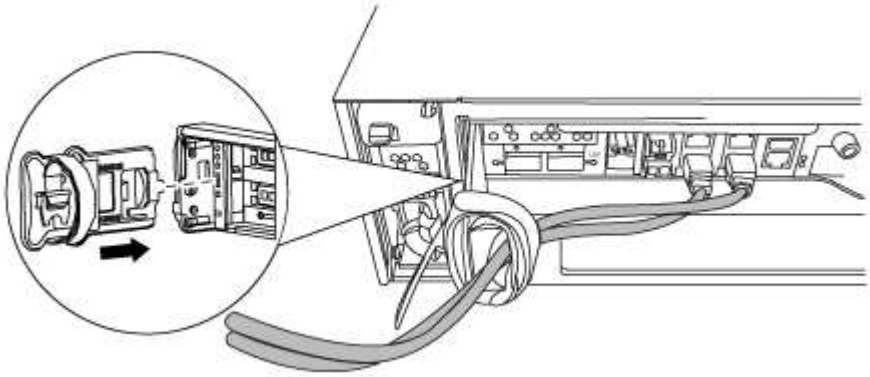
### Step 1: Open the controller module

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

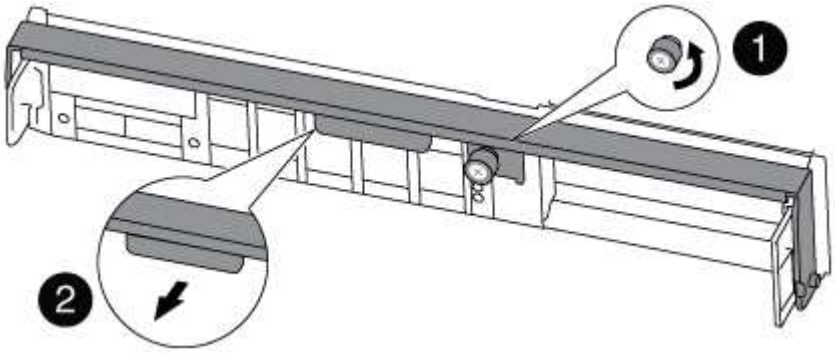
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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



4. If you left the SFP modules in the system after removing the cables, move them to the new controller module.
5. Loosen the thumbscrew on the cam handle on the controller module.




| | |
|---|---|
| 1 | Thumbscrew |

| | |
|---|---|
| ❷ | Cam handle |

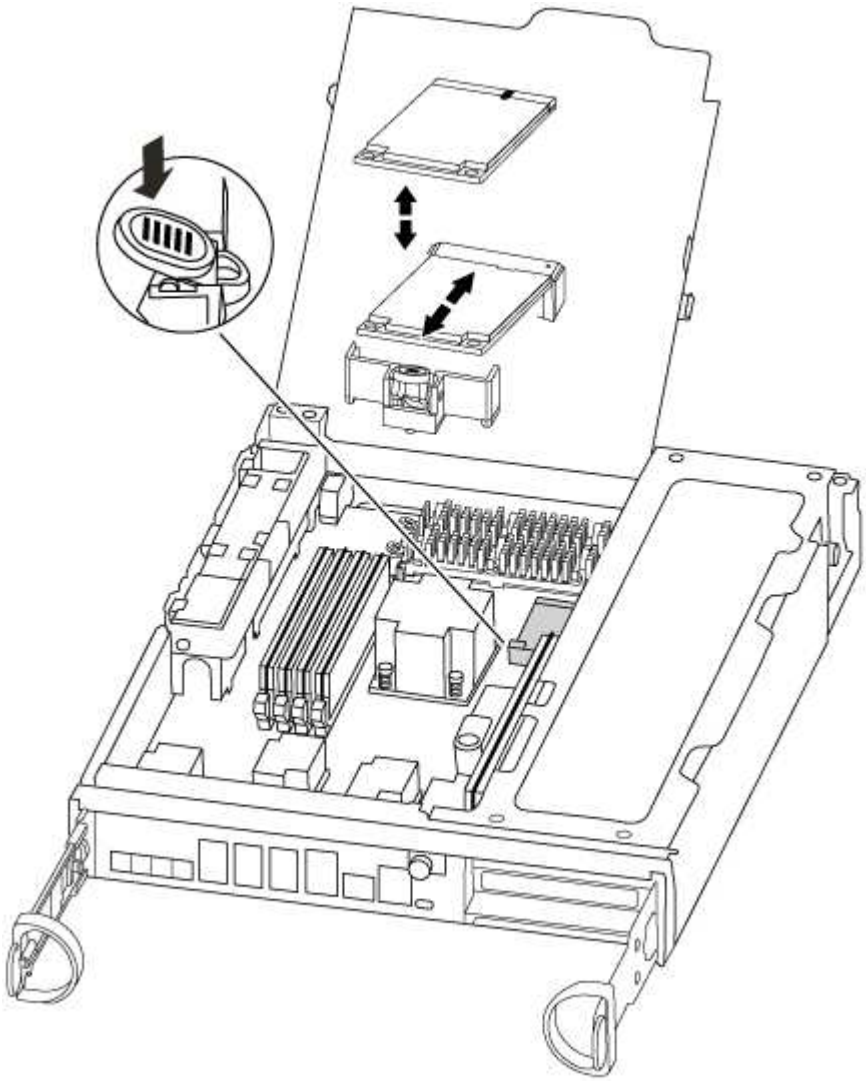
6. Pull the cam handle downward and begin to slide the controller module out of the chassis.

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

### Step 2: Move the boot device

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

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



2. Press the blue button on the boot media housing to release the boot media from its housing, and then gently pull it straight out of the boot media socket.

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

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

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

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

### Step 3: Move the NVMEM battery

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

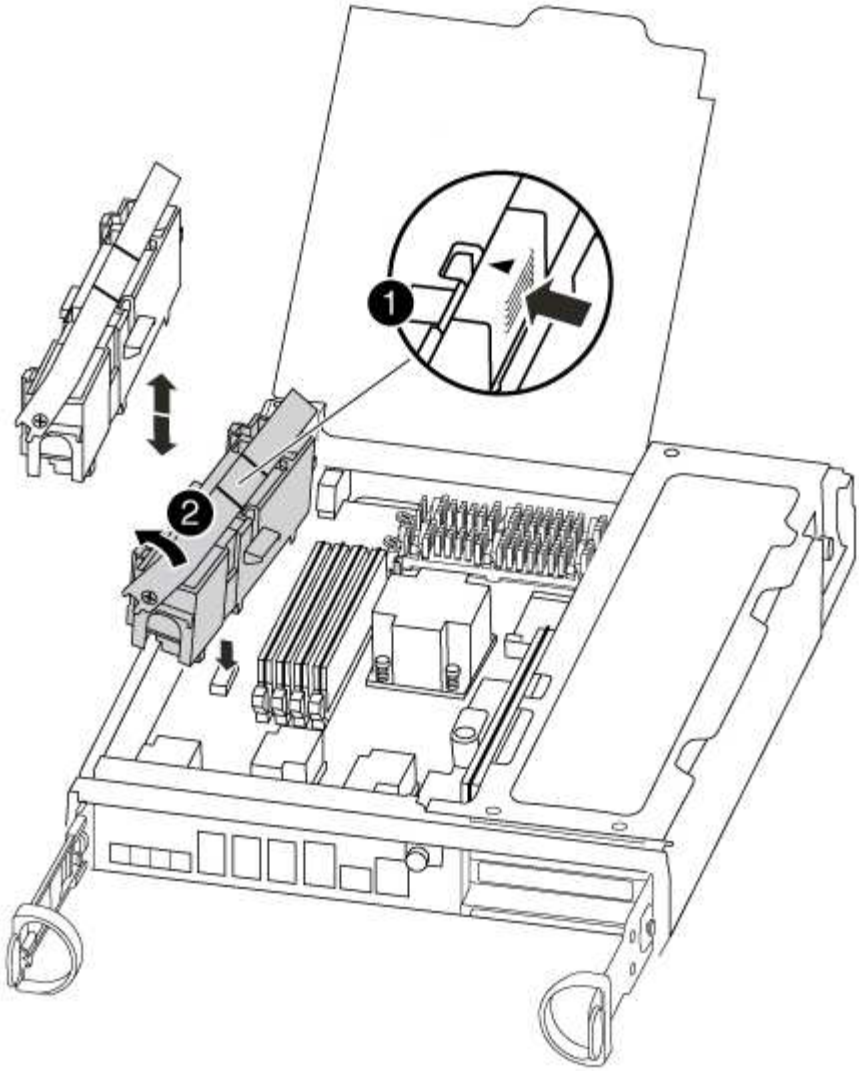
1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

> The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

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



| | |
|---|---|
| 1 | Battery lock tab |
| 2 | NVMEM battery pack |

3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Remove the battery from the controller module and set it aside.

**Step 4: Move the DIMMs**

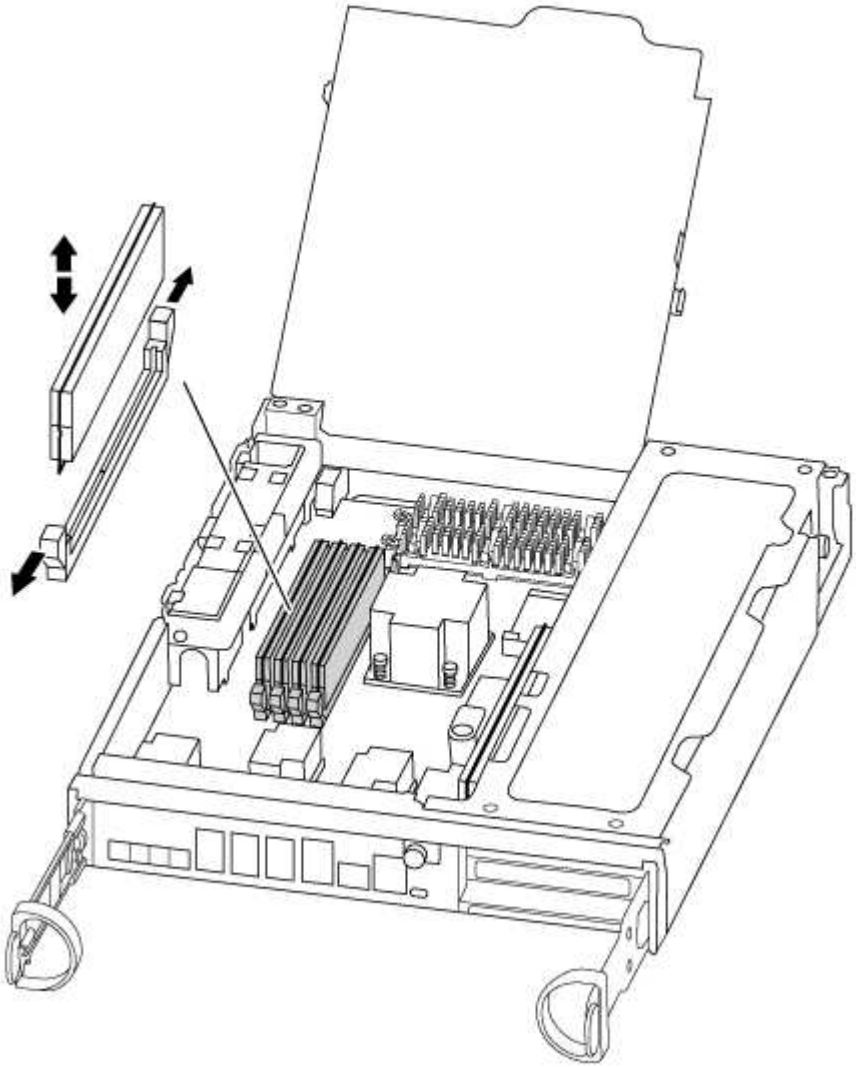
To move the DIMMs, locate and move them from the old controller into the replacement controller and follow the specific sequence of steps.

1. Locate the DIMMs on your controller module.
2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

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

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

The following illustration shows the location of system DIMMs:



4. Locate the slot where you are installing the DIMM.
5. Make sure that the DIMM ejector tabs on the connector are in the open position, and then insert the DIMM squarely into the slot.

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

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

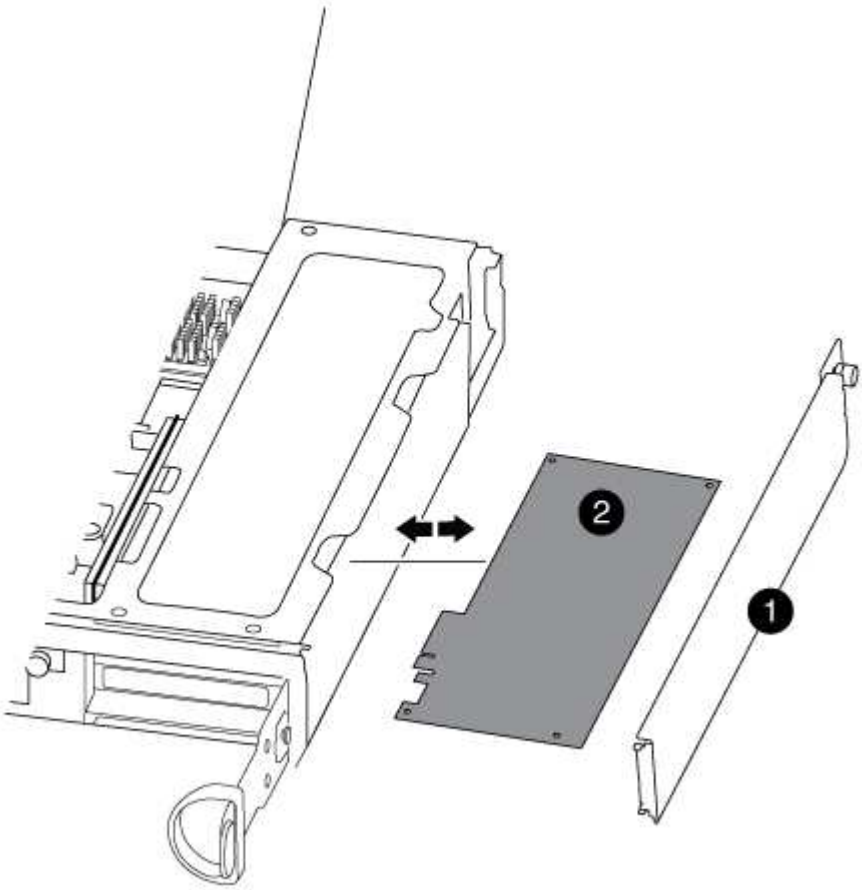
6. Repeat these steps for the remaining DIMMs.
7. Move the NVMEM battery to the replacement controller module.
8. Align the tab or tabs on the battery holder with the notches in the controller module side, and then gently push down on the battery housing until the battery housing clicks into place.

**Step 5: Move a PCIe card**

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

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

1. Loosen the thumbscrew on the controller module side panel.
2. Swing the side panel off the controller module.




| | |
|---|---|
| 1 | |
| Side panel | |
| 2 | |
| PCIe card | |

3. Remove the PCIe card from the old controller module and set it aside.

   Make sure that you keep track of which slot the PCIe card was in.

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

5. Open the new controller module side panel, if necessary, slide off the PCIe card filler plate, as needed, and carefully install the PCIe card.

   Be sure that you properly align the card in the slot and exert even pressure on the card when seating it in the socket. The card must be fully and evenly seated in the slot.

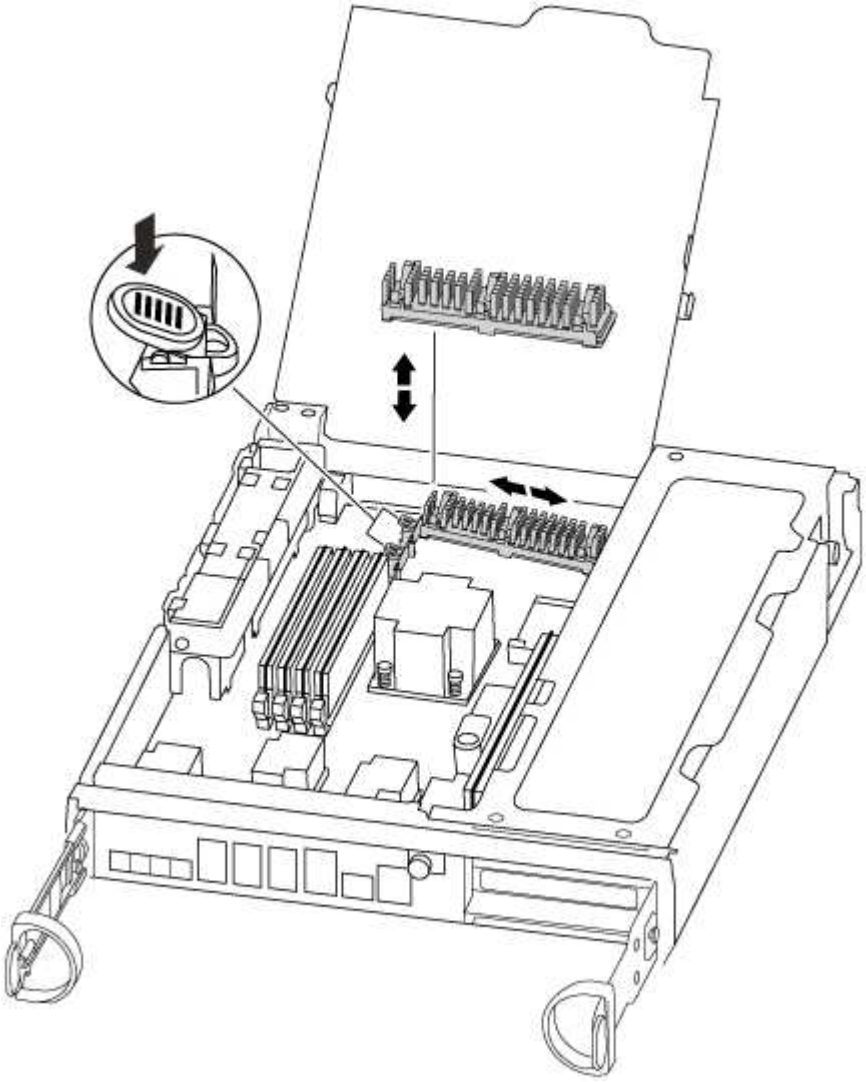
6. Repeat the preceding step for the remaining PCIe cards that you set aside.
7. Close the side panel and tighten the thumbscrew.

**Step 6: Move a caching module**

You must move the caching modules from the impaired controller modules to the replacement controller module when replacing a controller module.

1. Locate the caching module at the rear of the controller module and remove it:
   a. Press the release tab.
   b. Remove the heatsink.

      The storage system comes with two slots available for the caching module and only one slot is occupied, by default.



2. Move the caching module to the new controller module, and then align the edges of the caching module with the socket housing and gently push it into the socket.
3. Verify that the caching module is seated squarely and completely in the socket. If necessary, remove the caching module and reseat it into the socket.
4. Reseat and push the heatsink down to engage the locking button on the caching module housing.
5. Repeat the steps if you have a second caching module. Close the controller module cover.

**Step 7: Install the controller**

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

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.

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

   > 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:

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

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

**Important:** During the boot process, you might see the following prompts:

- A prompt warning of a system ID mismatch and asking to override the system ID.
- A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
  You can safely respond `y` to these prompts.

#### Restore and verify the system configuration - FAS8200

## 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 after replacing the controller

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

#### About this task

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

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

**Steps**

1. 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: `show date`

   The date and time are given in GMT.

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 HA state of the controller module

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

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

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

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

   - `ha`
   - `mcc`
   - `mcc-2n`
   - `mccip`
   - `non-ha`
3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

### Step 3: Run system-level diagnostics

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

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

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `halt`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

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

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

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

4. Run diagnostics as desired.

| If you want to run diagnostic tests on… | Then… |
| --- | --- |
| Individual components | a. Clear the status logs: `sldiag device clearstatus`<br>b. Display the available tests for the selected devices: `sldiag device show -dev` *`dev_name`*<br><br>*dev_name* can be any one of the ports and devices identified in the preceding step.<br><br>c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev` *`dev_name`* `-selection only`<br><br>-selection only disables all other tests that you do not want to run for the device.<br><br>d. Run the selected tests: `sldiag device run -dev` *`dev_name`*<br><br>After the test is complete, the following message is displayed:<br><br>`*> <SLDIAG:_ALL_TESTS_COMPLETED>`<br><br>e. Verify that no tests failed: `sldiag device status -dev` *`dev_name`* `-long -state failed`<br><br>System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component. |

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

5. Proceed based on the result of the preceding step.

| If the system-level diagnostics tests… | Then… |
| --- | --- |
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>`SLDIAG: No log messages are present.`<br>c. Exit Maintenance mode: `halt`<br>The system displays the LOADER prompt.<br>You have completed system-level diagnostics. |
| Resulted in some test failures | Determine the cause of the problem.<br>a. Exit Maintenance mode: `halt`<br>b. Perform a clean shutdown, and then disconnect the power supplies.<br>c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Reconnect the power supplies, and then power on the storage system.<br>e. Rerun the system-level diagnostics test. |

#### Recable the system and reassign disks - FAS8200

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

### Step 1: Recable the system

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

**Steps**

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.

d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

### Step 2: Reassign disks

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. You must use the correct procedure for your configuration.

#### Option 1: Verify the system ID change on an HA system

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

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

1. If the *replacement* controller 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* controller, boot the controller, 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* controller console and then, from the healthy controller, 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 controller, 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`
                                       Takeover
   Node              Partner           Possible     State Description
   ------------      ------------      --------
   -------------------------------------
   node1             node2             false        System ID changed on
   partner (Old:
                                                   151759755, New:
   151759706), In takeover
   node2             node1             -            Waiting for giveback
   (HA mailboxes)
   ```

4. From the healthy controller, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

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

   b. Save any coredumps: `system node run -node local-node-name partner savecore`
   c. Wait for `savecore` command to complete before issuing the giveback.

You can enter the following command to monitor the progress of the `savecore` command: `system node run -node local-node-name partner savecore -s`

d. Return to the admin privilege level: `set -privilege admin`

5. Give back the controller:

a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode replacement_node_name`

The *replacement* controller 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 content 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* controller 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 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

#### Option 2: 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) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

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

   You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

   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   system-1  (118065481) Pool0  J8Y0TDZC       system-1
(118065481)
disk_name   system-1  (118065481) Pool0  J8Y09DXC       system-1
(118065481)
.
.
.
```

6. From the healthy node, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

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

   b. Verify that the coredumps are saved: `system node run -node` *`local-node-name`* `partner savecore`

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

   c. Return to the admin privilege level: `set -privilege admin`
7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
8. Boot the *replacement* node: `boot_ontap`
9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`
10. Verify the MetroCluster configuration: `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 - FAS8200

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

### Step 1: Install licenses for the replacement controller in ONTAP

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

#### About this task

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

#### Before you begin

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.

#### 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: Restore Storage and Volume Encryption functionality

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

**Step**

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use 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

### Step 3: Verify LIFs and register the serial number

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

**Steps**

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

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

2. Register the system serial number with NetApp Support.
   - 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. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

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

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

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 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 & Replacements page for further information.

### Replace a DIMM - FAS8200

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

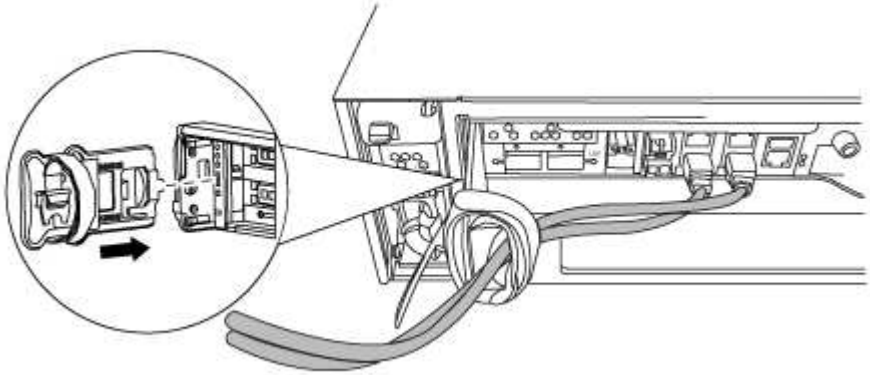
**Step 2: Open the controller module**

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.

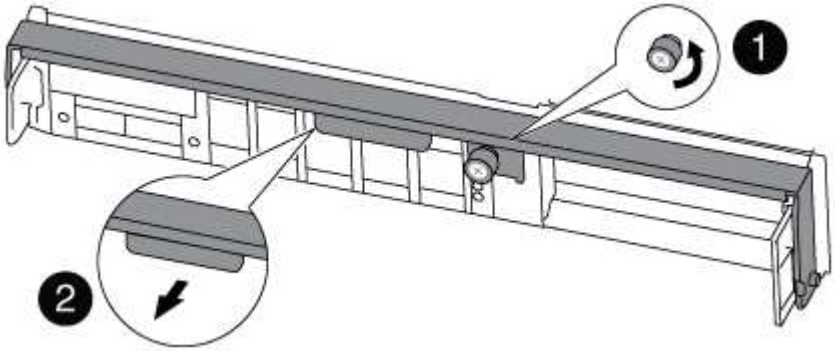
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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



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




| | |
|---|---|
| 1 | Thumbscrew |
| 2 | Cam handle |

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

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

#### Step 3: Replace the DIMMs

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

1. Check the NVMEM LED on the controller module.

   You must perform a clean system shutdown before replacing system components to avoid losing unwritten data in the nonvolatile memory (NVMEM). The LED is located on the back of the controller module. Look for the following icon:

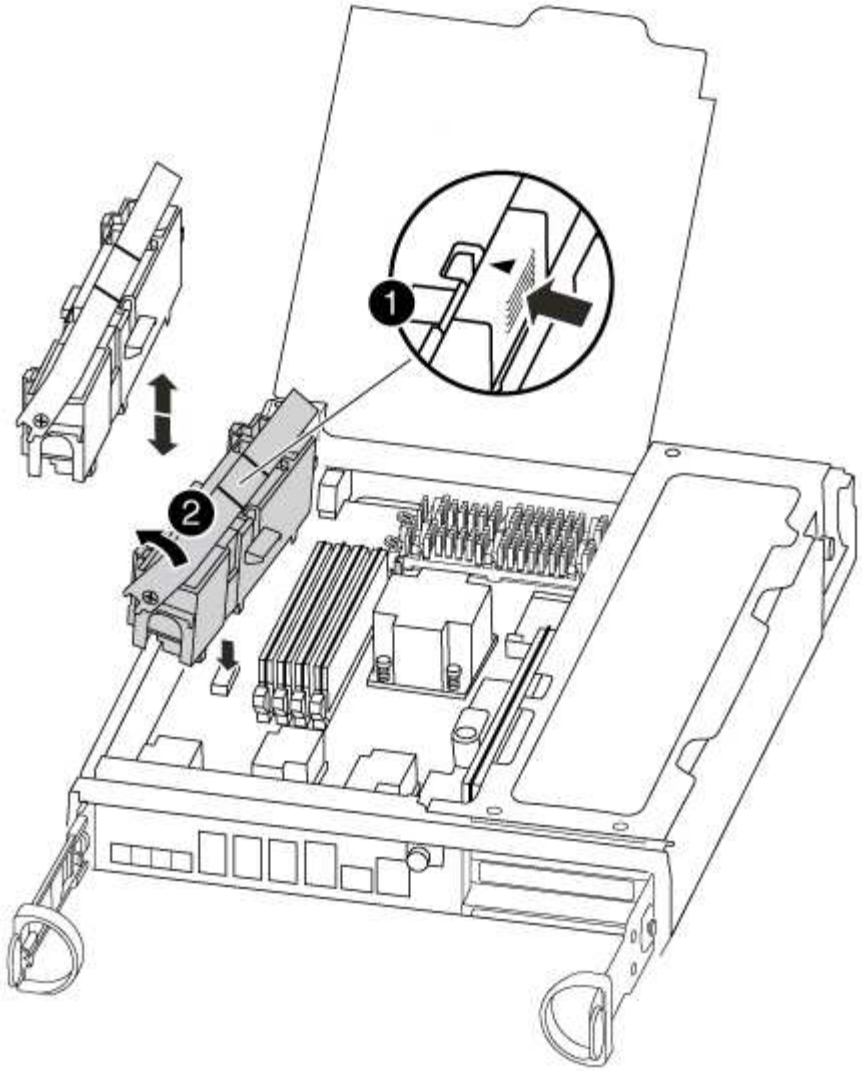
2. If the NVMEM LED is not flashing, there is no content in the NVMEM; you can skip the following steps and proceed to the next task in this procedure.
3. Unplug the battery:

   > The NVMEM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

   - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
   - If the LED is on and power is on, unwritten data is stored on NVMEM.

     This typically occurs during an uncontrolled shutdown after Data ONTAP has successfully booted.

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



| | |
|---|---|
| 1 | NVMEM battery lock tab |
| 2 | NVMEM battery |

b. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.

c. Wait a few seconds, and then plug the battery back into the socket.

4. Check the NVMEM LED on the controller module.
5. Locate the DIMMs on your controller module.

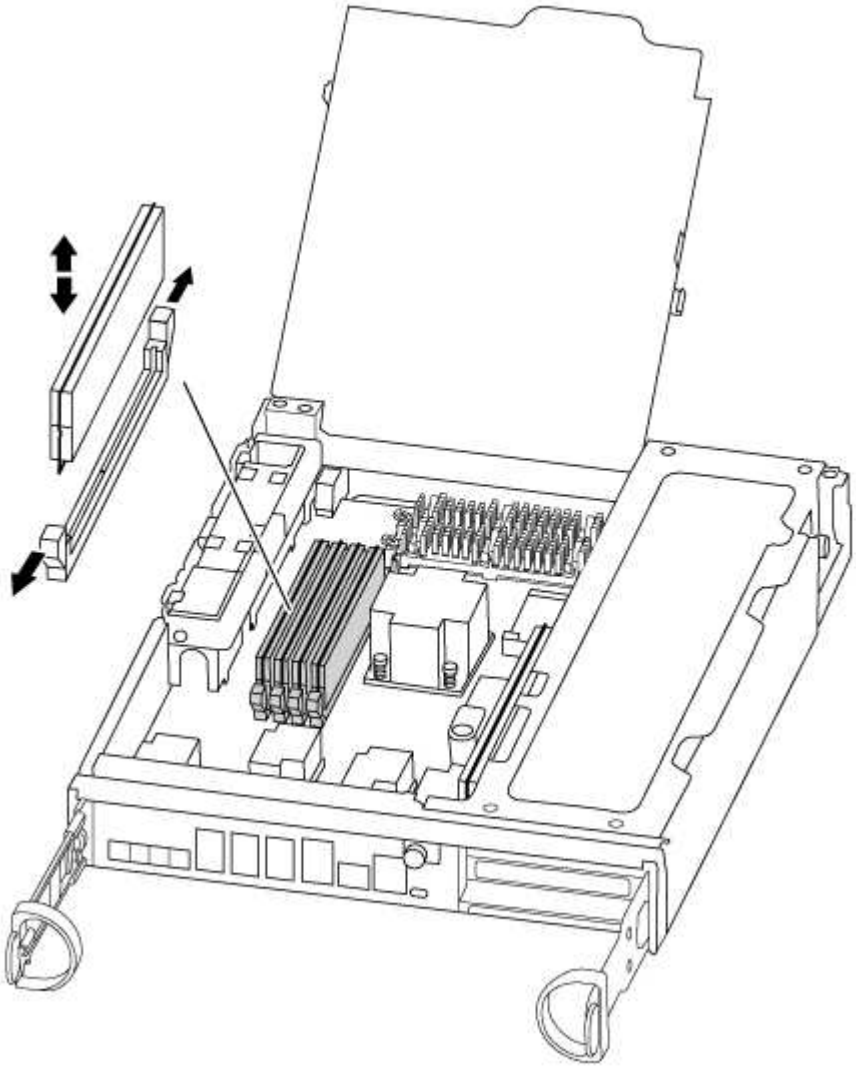
> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.

6. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
7. 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.

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

The following illustration shows the location of system DIMMs:



8. 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.

9. 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.

10. 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.

11. Locate the NVMEM battery plug socket, and then squeeze the clip on the face of the battery cable plug to insert it into the socket.

    Make sure that the plug locks down onto the controller module.

12. Close the controller module cover.

#### Step 4: Reinstall the controller

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it to a state where you can run diagnostic tests on the replaced component.

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 system, as needed.

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

3. Complete the reinstallation of the controller module:

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

   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

   b. Tighten the thumbscrew on the cam handle on back of the controller module.
   c. If you have not already done so, reinstall the cable management device.
   d. Bind the cables to the cable management device with the hook and loop strap.
   e. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.
   f. Select the option to boot to Maintenance mode from the displayed menu.

#### Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.

b. After the controller boots to Maintenance mode, halt the controller: `halt`

After you issue the command, you should wait until the system stops at the LOADER prompt.

> During the boot process, you can safely respond `y` to prompts:

- A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

| If the system-level diagnostics tests… | Then… |
|---|---|
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>SLDIAG: No log messages are present.<br>c. Exit Maintenance mode: `halt`<br>The controller displays the LOADER prompt.<br>d. Boot the controller from the LOADER prompt: `bye`<br>e. Return the controller to normal operation: |

| If your controller is in… | Then… |
|---|---|
| An HA pair | Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`*<br>If you disabled automatic giveback, re-enable it with the storage failover modify command. |

| If your controller is in… | Then… |
| --- | --- |
| A two-node MetroCluster configuration | Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process. |
| A stand-alone configuration | Proceed to the next step. No action is required. You have completed system-level diagnostics. |
| Resulted in some test failures | Determine the cause of the problem:<br>a. Exit Maintenance mode: `halt`<br>After you issue the command, wait until the system stops at the LOADER prompt.<br>b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis:<br>◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module.<br>◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources.<br>c. Verify that you have observed all the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu:<br>◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis.<br>The controller module boots up when fully seated.<br>◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on.<br>e. Select Boot to maintenance mode from the menu.<br>f. Exit Maintenance mode by entering the following command: `halt`<br>After you issue the command, wait until the system stops at the LOADER prompt.<br>g. Rerun the system-level diagnostic test. |

#### Step 6 (Two-node MetroCluster only): Switch back aggregates

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

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 7: 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 & Replacements page for further information.

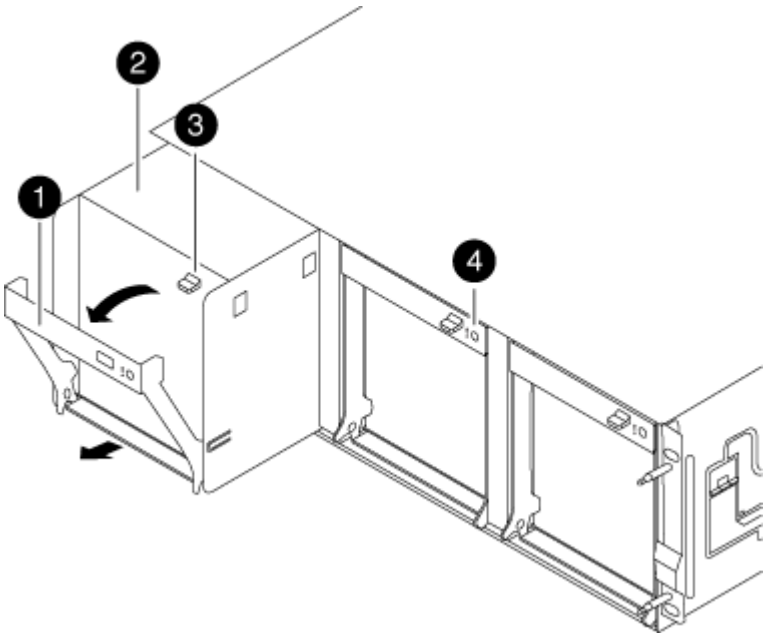
### Swap out a fan - FAS8200

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.

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 down the release latch on the fan module cam handle, and then pull the cam handle downward.

   The fan module moves a little bit away from the chassis.




| | |
|---|---|
| 1 | Cam handle |
| 2 | Fan module |

| | |
|---|---|
| ❸ | Cam handle release latch |
| ❹ | Fan module Attention LED |

5. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

> 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.

6. Set the fan module aside.
7. Insert the replacement fan module into the chassis by aligning it with the opening, and then sliding it into the chassis.
8. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

9. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The fan LED should be green after the fan is seated and has spun up to operational speed.

10. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.
11. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Replace the NVMEM battery - FAS8200

To replace an NVMEM battery in the system, you must remove the controller module from the system, open it, replace the battery, and close and replace the controller module.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

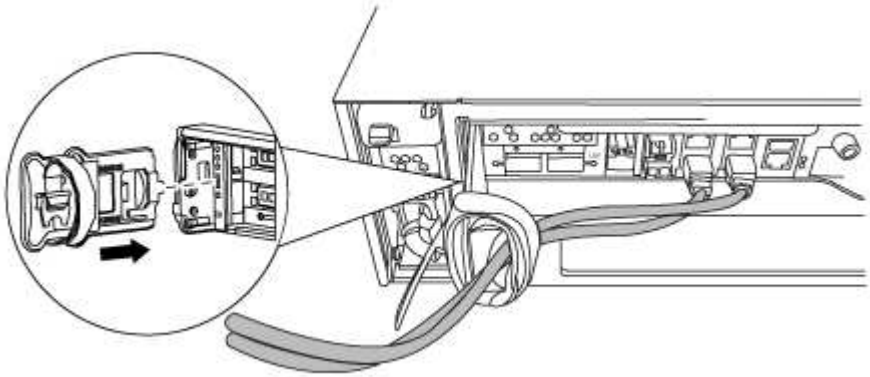
**Step 2: Open the controller module**

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.

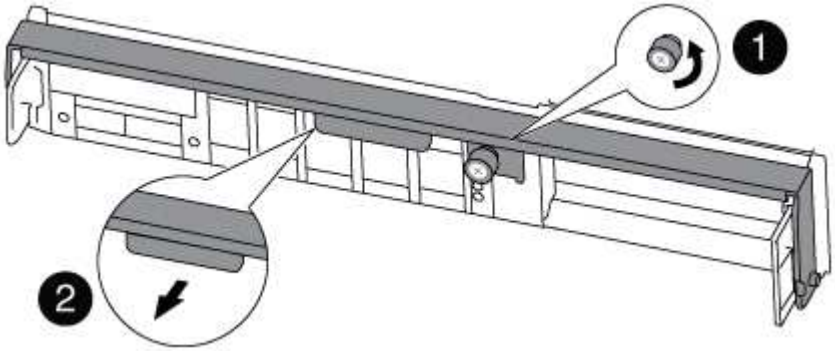
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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



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




| | |
|---|---|
| 1 | Thumbscrew |
| 2 | Cam handle |

5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

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

#### Step 3: Replace the NVMEM battery

To replace the NVMEM battery in your system, you must remove the failed NVMEM battery from the system and replace it with a new NVMEM battery.

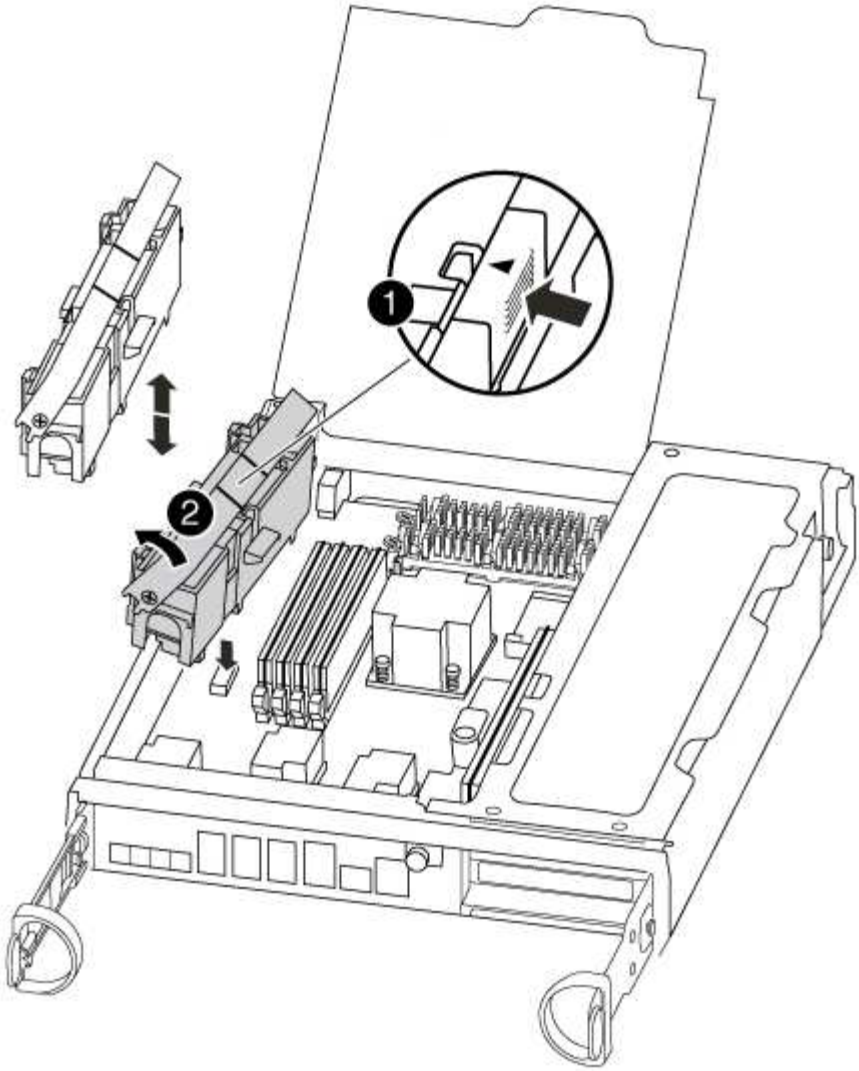
1. Check the NVMEM LED:
   - If your system is in an HA configuration, go to the next step.
   - If your system is in a stand-alone configuration, cleanly shut down the controller module, and then check the NVRAM LED identified by the NV icon.

     > The NVRAM LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

     - If power is lost without a clean shutdown, the NVMEM LED flashes until the destage is complete, and then the LED turns off.
     - If the LED is on and power is on, unwritten data is stored on NVMEM.

       This typically occurs during an uncontrolled shutdown after ONTAP has successfully booted.

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



| | |
|---|---|
| 1 | Battery lock tab |
| 2 | NVMEM battery pack |

3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
4. Remove the replacement battery from its package.
5. Align the tab or tabs on the battery holder with the notches in the controller module side, and then gently push down on the battery housing until the battery housing clicks into place.
6. Close the CPU air duct.

   Make sure that the plug locks down to the socket.

#### Step 4: Reinstall the controller

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and boot it to a state where you can run diagnostic tests on the replaced component.

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 system, as needed.

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

3. Complete the reinstallation of the controller module:

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

   a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.

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

   b. Tighten the thumbscrew on the cam handle on back of the controller module.
   c. If you have not already done so, reinstall the cable management device.
   d. Bind the cables to the cable management device with the hook and loop strap.
   e. As each controller starts the booting, press `Ctrl-C` to interrupt the boot process when you see the message `Press Ctrl-C for Boot Menu`.
   f. Select the option to boot to Maintenance mode from the displayed menu.

#### Step 5: Run system-level diagnostics

After installing a new NVMEM battery, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the controller boots to Maintenance mode, halt the controller: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      > During the boot process, you can safely respond `y` to prompts:

      - A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the NVMEM memory: `sldiag device run -dev nvmem`
4. Verify that no hardware problems resulted from the replacement of the NVMEM battery: `sldiag device status -dev nvmem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

| If the system-level diagnostics tests… | Then… |
|---|---|
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>SLDIAG: No log messages are present.<br>c. Exit Maintenance mode: `halt`<br>The controller displays the LOADER prompt.<br>d. Boot the controller from the LOADER prompt: `bye`<br>e. Return the controller to normal operation: |

| If your controller is in… | Then… |
|---|---|
| An HA pair | Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`*<br>If you disabled automatic giveback, re-enable it with the storage failover modify command. |
| A two-node MetroCluster configuration | Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process. |
| A stand-alone configuration | Proceed to the next step. No action is required. You have completed system-level diagnostics. |

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

#### Step 6: Switch back aggregates in a two-node MetroCluster configuration

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

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 7: 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 & Replacements page for further information.

### Replace a PCIe card - FAS8200

To replace a PCIe card, 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 are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Returning SEDs to unprotected mode" section of the *ONTAP 9 NetApp Encryption Power Guide*.

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

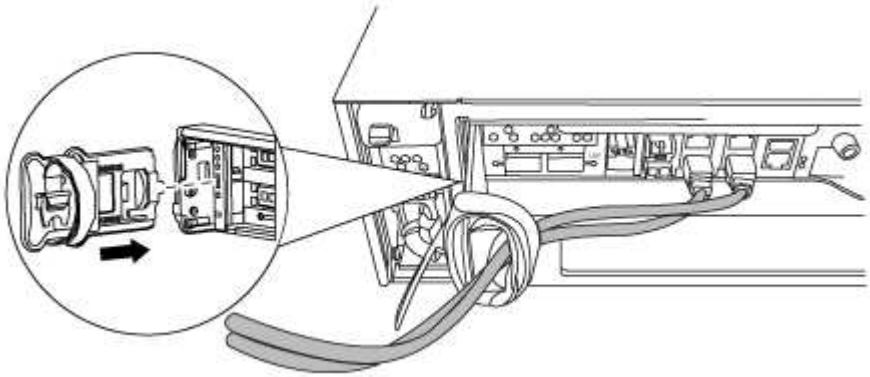
**Step 2: Open the controller module**

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.

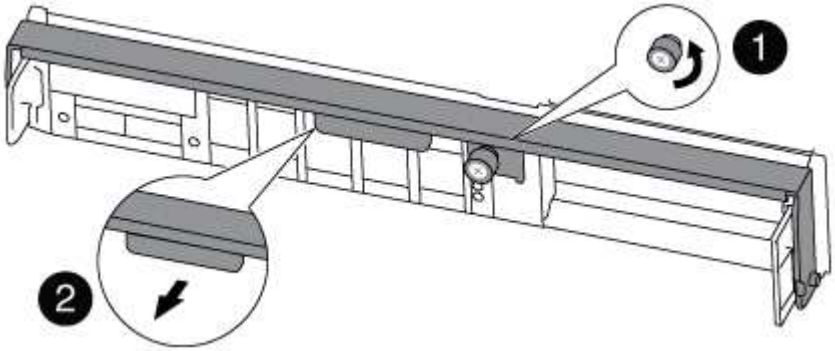
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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



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




| | |
|---|---|
| 1 | Thumbscrew |
| 2 | Cam handle |

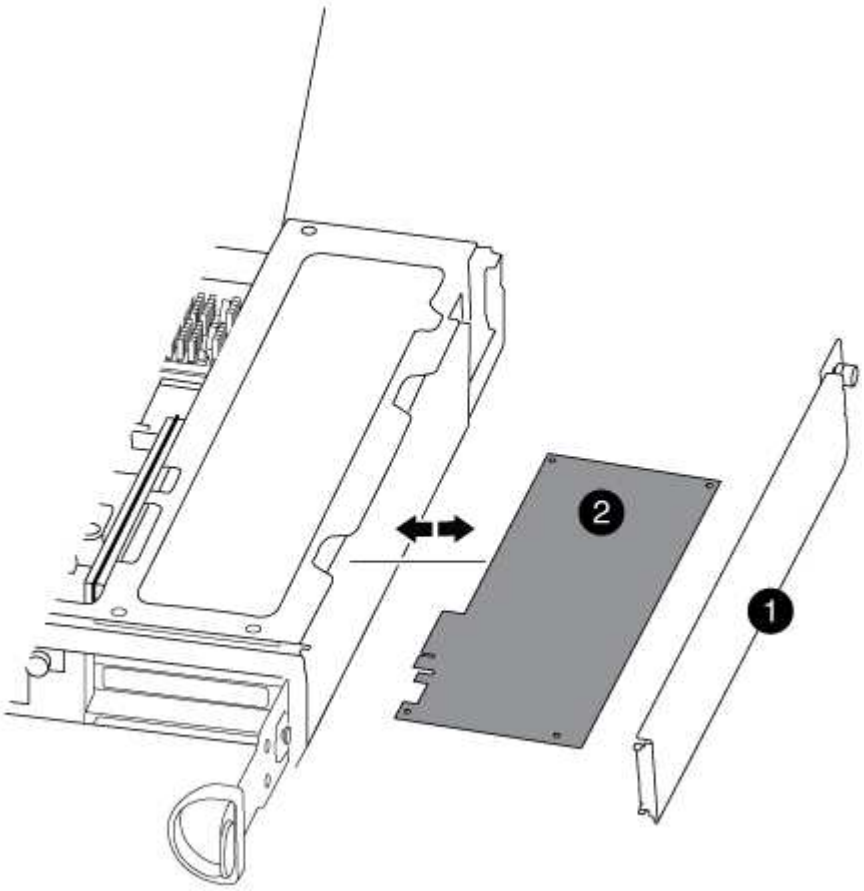
5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

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

#### Step 3: Replace a PCIe card

To replace a PCIe card, locate it within the controller and follow the specific sequence of steps.

1. Loosen the thumbscrew on the controller module side panel.
2. Swing the side panel off the controller module.




| | |
|---|---|
| 1 | Side panel |
| 2 | PCIe card |

3. Remove the PCIe card from the controller module and set it aside.
4. Install the replacement PCIe card.

   Be sure that you properly align the card in the slot and exert even pressure on the card when seating it in the socket. The PCIe card must be fully and evenly seated in the slot.

   > If you are installing a card in the bottom slot and cannot see the card socket well, remove the top card so that you can see the card socket, install the card, and then reinstall the card you removed from the top slot.

5. Close the side panel and tighten the thumbscrew.

#### Step 4: Reinstall the controller

After you replace a component within the controller module, you must reinstall the controller module in the system chassis and 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 system, as needed.

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

3. Complete the reinstallation of the controller module:

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

| If your system is in… | Then perform these steps… |
|---|---|
| An HA pair | a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module.<br>> Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. If you have not already done so, reconnect the cables to the controller module.<br>d. Bind the cables to the cable management device with the hook and loop strap. |
| A two-node MetroCluster configuration | a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position. Tighten the thumbscrew on the cam handle on back of the controller module.<br>> Do not use excessive force when sliding the controller module into the chassis to avoid damaging the connectors.<br>b. If you have not already done so, reinstall the cable management device.<br>c. If you have not already done so, reconnect the cables to the controller module.<br>d. Bind the cables to the cable management device with the hook and loop strap.<br>e. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process. |

4. 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.

5. Return the controller to normal operation:

| If your system is in… | Issue this command from the partner's console… |
|---|---|
| An HA pair | `storage failover giveback -ofnode` *`impaired_node_name`* |
| A two-node MetroCluster configuration | Proceed to the next step. The MetroCluster switchback procedure is done in the next task in the replacement process. |

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

#### Step 5 (two-node MetroCluster only): Switch back aggregate

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

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 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 & Replacements page for further information.

### Swap out a power supply - FAS8200

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.

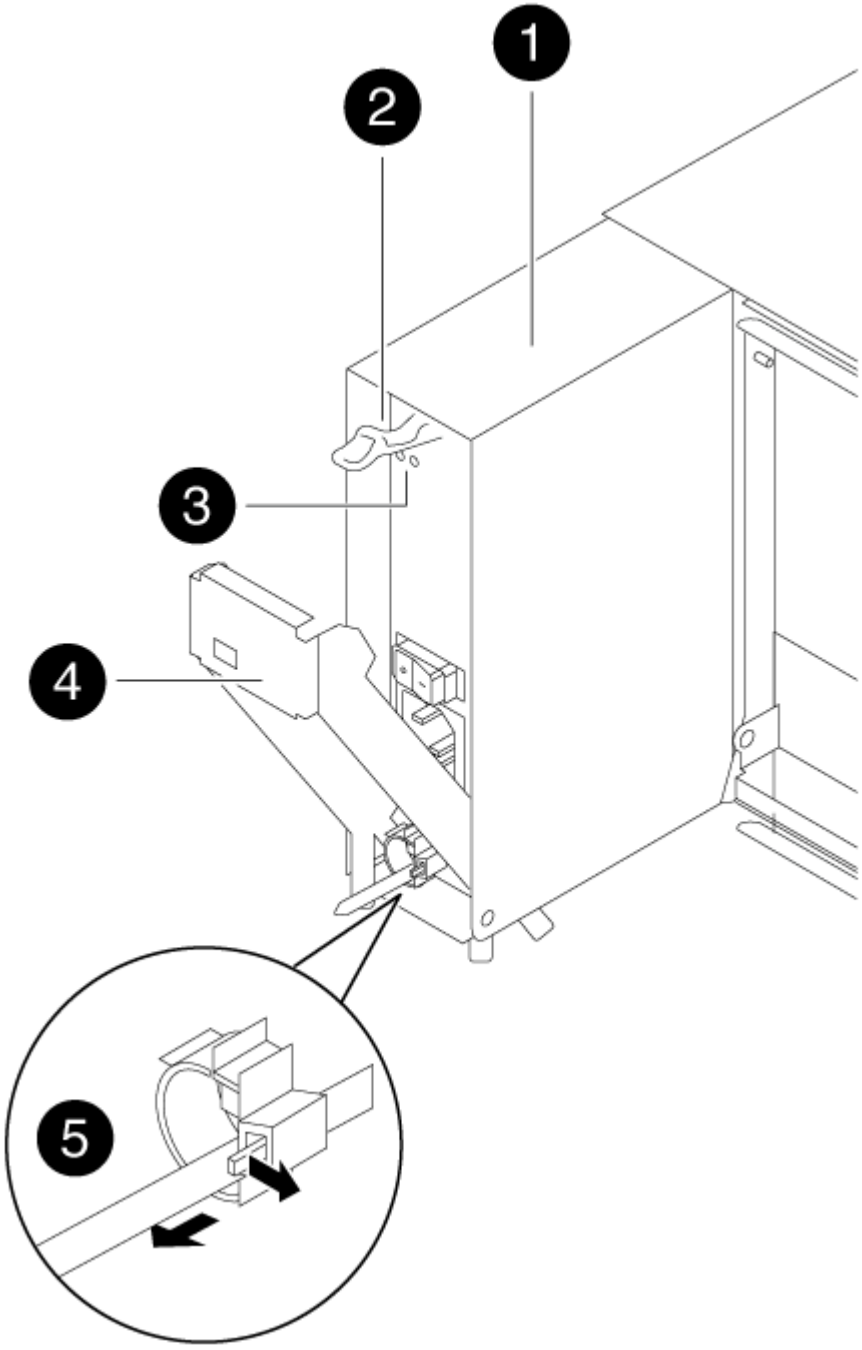
All other components in the system must be functioning properly; if not, you must contact technical support.

- The power supplies are redundant and hot-swappable.
- 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.

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 down the release latch on the power supply cam handle, and then lower the cam handle to the fully open position to release the power supply from the mid plane.



| | |
|---|---|
| 1 | Power supply |
| 2 | Cam handle release latch |
| 3 | Power and Fault LEDs |
| 4 | Cam handle |
| 5 | Power cable locking mechanism |

5. Use the cam handle to slide the power supply out of the system.

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

6. Make sure that the on/off switch of the new power supply is in the Off position.
7. 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 using the cam handle.

   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.

8. Push firmly on the power supply cam handle to seat it all the way into the chassis, and then push the cam handle to the closed position, making sure that the cam handle release latch clicks into its locked position.
9. 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.

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

   The power supply LEDs are lit when the power supply comes online.

2. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

**Replace the real-time clock battery - FAS8200**

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.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

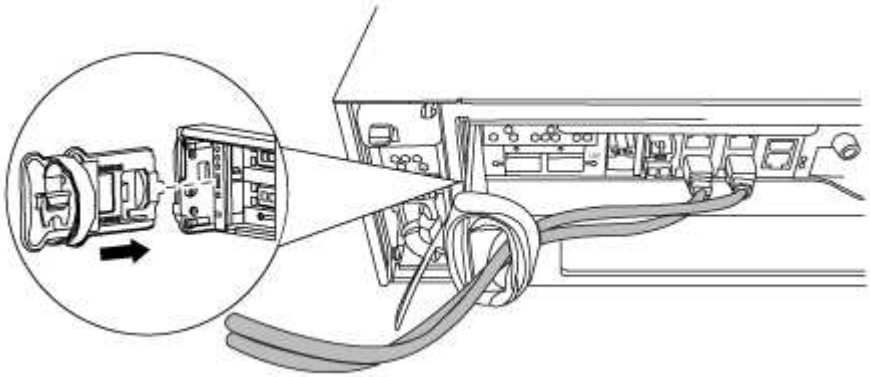
**Step 2: Open the controller module**

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.

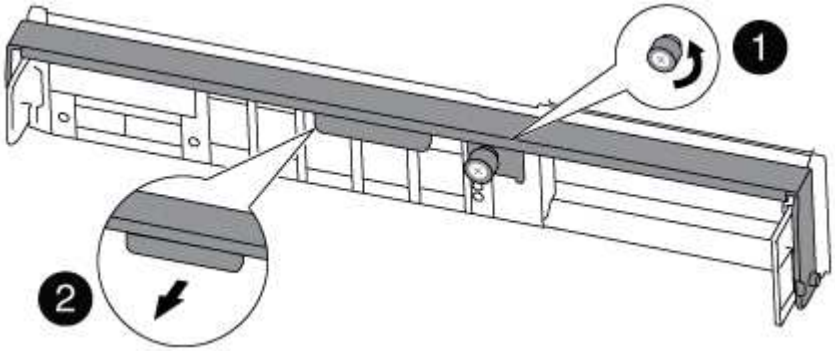
1. If you are not already grounded, properly ground yourself.
2. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

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



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




| | |
|---|---|
| 1 | Thumbscrew |
| 2 | Cam handle |

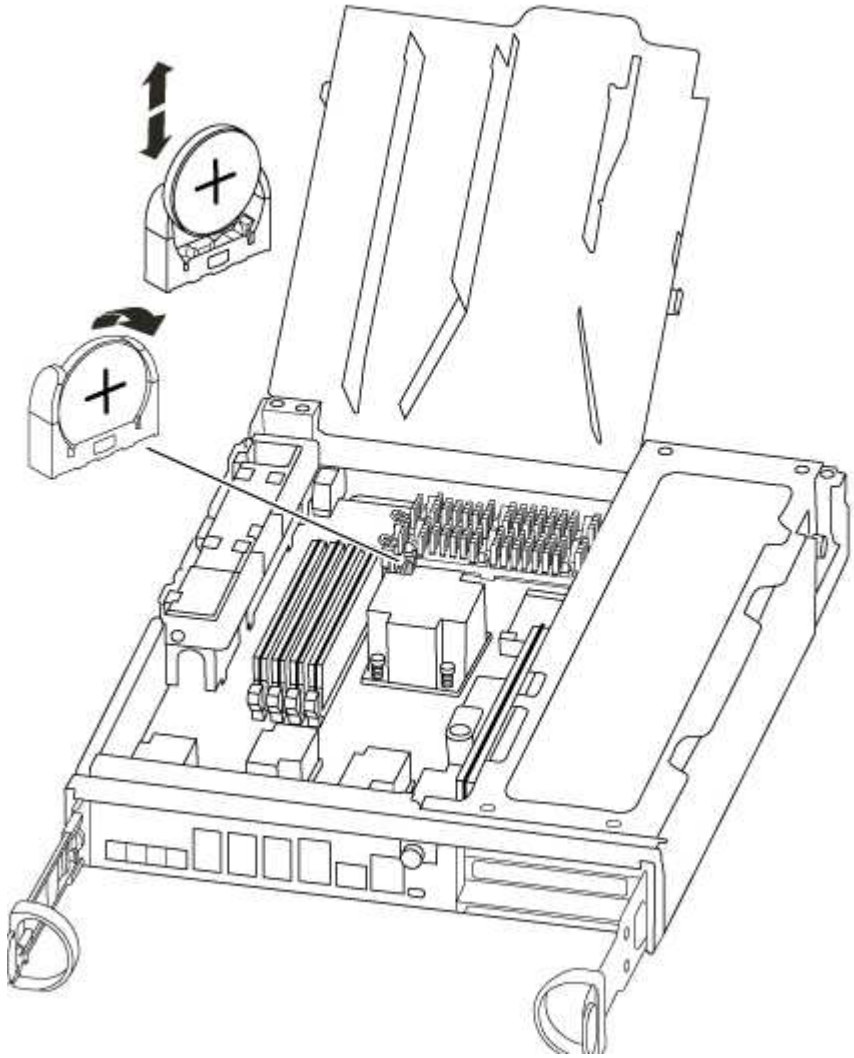
5. Pull the cam handle downward and begin to slide the controller module out of the chassis.

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

**Step 3: Replace the RTC Battery**

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

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



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.

#### Step 4: Reinstall the controller module and setting time/date after RTC battery replacement

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.

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.

      Tighten the thumbscrew on the cam handle on back of the controller module.

      > 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 controller with the `show date` command.
   b. At the LOADER prompt on the target controller, 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 controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller 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

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

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 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 & Replacements page for further information.

# FAS8300 and FAS8700 System Documentation

## Install and setup

#### Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

For MetroCluster configurations, see either:

- Install MetroCluster IP configuration
- Install MetroCluster Fabric-Attached configuration

#### Quick guide - FAS8300 and FAS8700

This guide gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

FAS8300 and FAS8700 Installation and Setup Instructions

### Videos - FAS8300 and FAS8700

There are two videos; one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

#### Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

FAS8300 and FAS8700 Installation and setup instructions

#### Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

### Detailed guide - FAS8300 and FAS8700

This guide gives detailed step-by-step instructions for installing a typical NetApp system. Use this guide if you want more detailed installation instructions.

#### Step 1: Prepare for installation

To install your system, you need to create an account, register the system, and get license keys. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

You need to have access to the Hardware Universe for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

NetApp Hardware Universe

Find the Release Notes for your version of ONTAP 9

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser

**Steps**

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Inventory and make a note of the number and types of cables you received.

The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the Hardware Universe to locate the cable and identify its use.

NetApp Hardware Universe

| Type of cable… | Part number and length | Connector type | For… |
|---|---|---|---|
| 100 GbE cable (QSF(28) | X66211A-05 (112-00595), 0.5m<br>X66211A-1 (112-00573), 1m<br>X66211A-2 (112-00574), 2m<br>X66211A-5 (112-00574), 5m | | Storage, cluster interconnect/HA, and Ethernet data (order-dependent) |
| 25 GbE cable (SFP28s) | X66240-2 (112-00598), 2m<br>X66240-5 (112-00639), 5m | | GbE network connection (order-dependent) |
| 32 Gb FC (SFP+ Op) | X66250-2 (112-00342), 2m<br>X66250-5 (112-00344), 5m<br>X66250-15 (112-00346), 15m | | FC network connection |
| Storage Cables | X66030A (112-00435), .5m<br>X66031A (112-00436), 1m<br>X66032A (112-00437), 2m<br>X66033A (112-00438), 3m | | mini-SAS HD to mini-SAS HD cables (order-dependent) |
| Optical cables | X66250-2-N-C (112-00342) | | 16 Gb FC or 25GbE cables for mezzanine cards (order-dependent) |
| RJ-45 (order dependent) | X6585-R6 (112-00291), 3m<br>X6562-R6 (112-00196), 5m | | Management network |
| Micro-USB console cable | Not applicable | | Console connection used during software setup if laptop or console does not support network discovery. |
| Power cables | Not applicable | | Powering up the system |

4. Review the *NetApp ONTAP Confiuration Guide* and collect the required information listed in that guide.

   ONTAP Configuration Guide

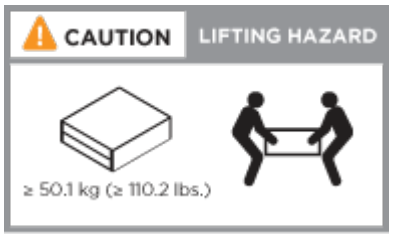
#### Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

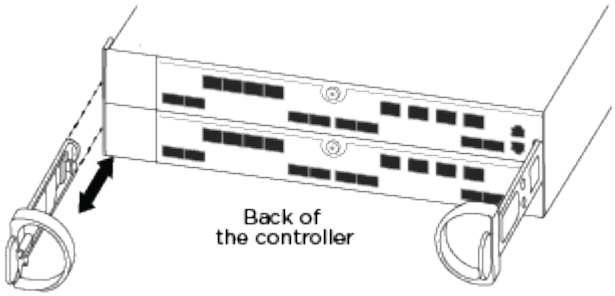
**Steps**

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

   You need to be aware of the safety concerns associated with the weight of the system.




3. Attach cable management devices (as shown).




4. Place the bezel on the front of the system.

#### Step 3: Cable controllers to your network

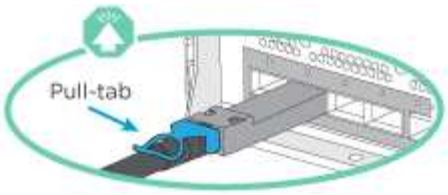
You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

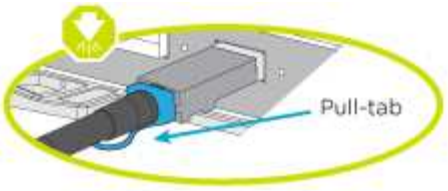
**Option 1: Cable a two-node switchless cluster**

The optional data ports, optional NIC cards, and management ports on the controller modules are connected to switches. The cluster interconnect and HA ports are cabled on both controller modules.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all onboard ports and down for expansion (NIC) cards.



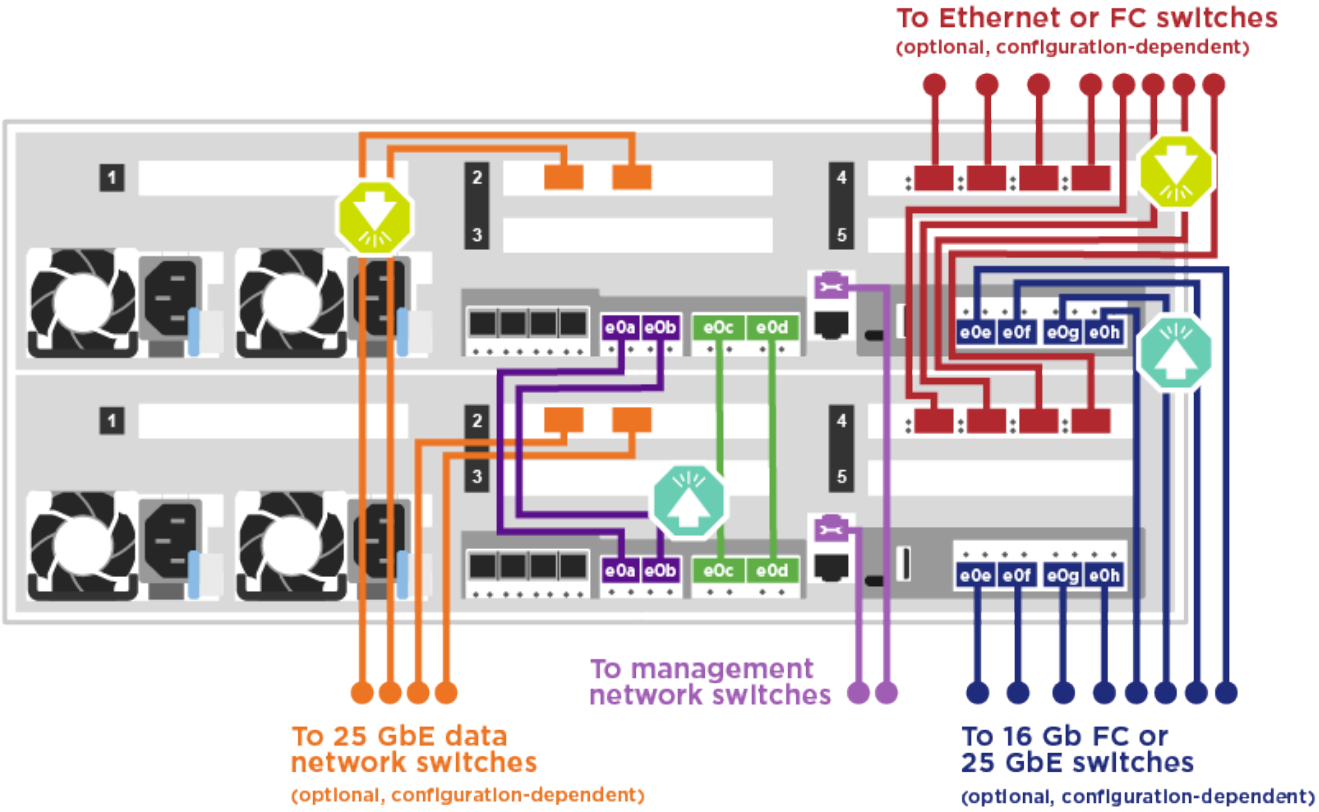




As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Two-node switchless cluster cabling



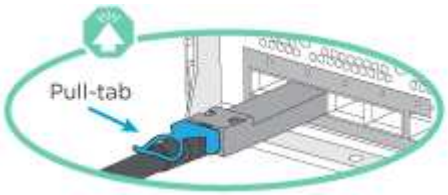

2. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

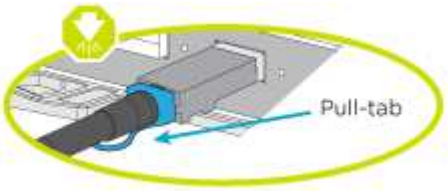
**Option 2: Cable a switched cluster**

The optional data ports, optional NIC cards, mezzanine cards, and management ports on the controller modules are connected to switches. The cluster interconnect and HA ports are cabled on to the cluster/HA switch.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all onboard ports and down for expansion (NIC) cards.



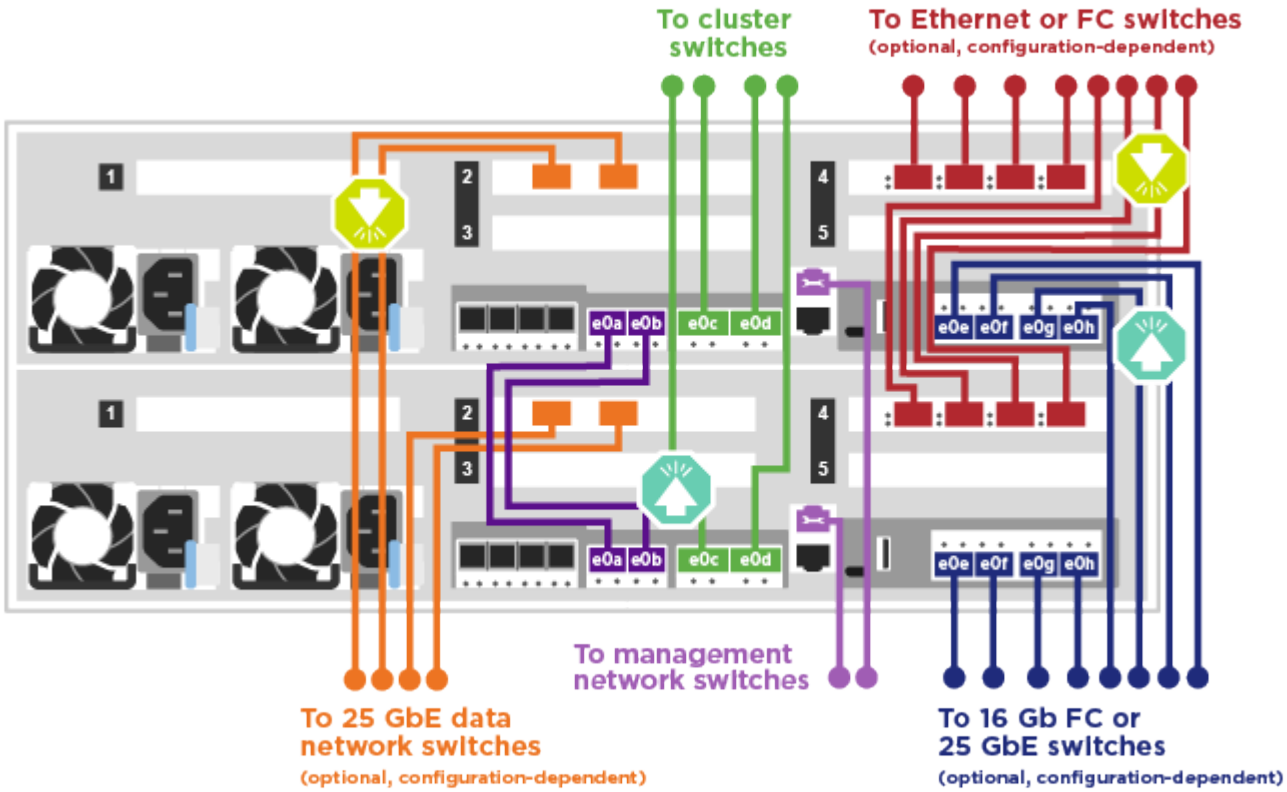




As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Switched cluster cabling

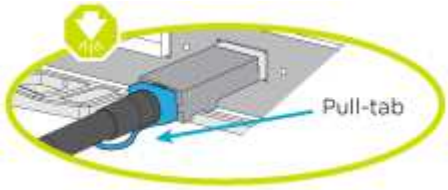



2. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

### Option 1: Cable the controllers to SAS drive shelves

You must cable each controller to the IOM modules on both SAS drive shelves.

Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the DS224-C are down.

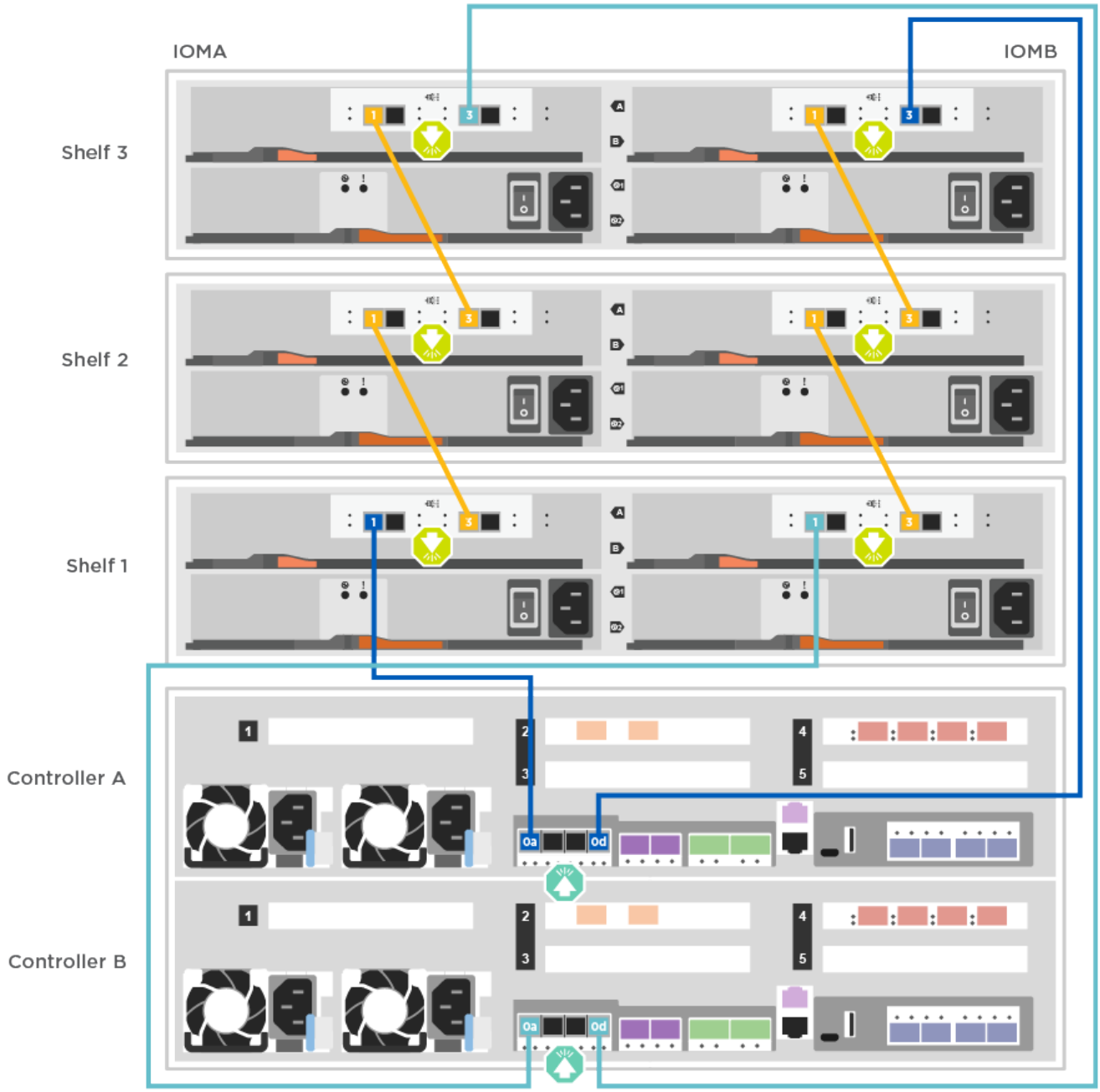



> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. Use the following animation or illustration to cable your controllers to two drive shelves.

   Cabling the controllers to SAS drive shelves




2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

#### Step 5: Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

#### Option 1: Completing system setup and configuration if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

#### Steps

1. Use the following animation to set one or more drive shelf IDs:

   Setting drive shelf IDs

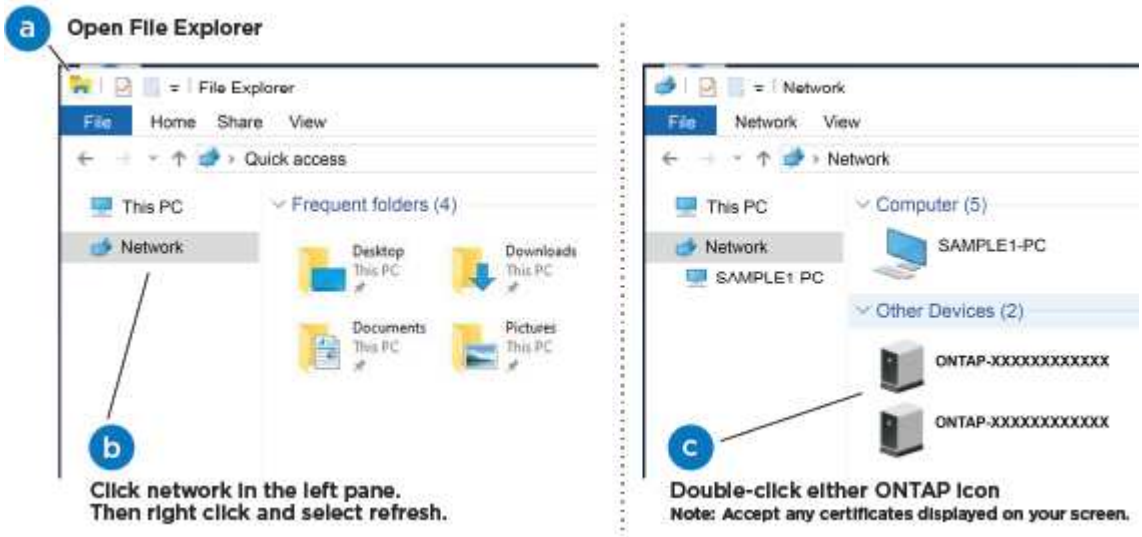
2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

4. Use the following animation to connect your laptop to the Management switch.

   Connecting your laptop to the Management switch

5. Select an ONTAP icon listed to discover:




   a. Open File Explorer.
   b. Click network in the left pane.
   c. Right click and select refresh.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

      XXXXX is the system serial number for the target node.

   System Manager opens.

6. Use System Manager guided setup to configure your system using the data you collected in the *NetApp ONTAP Configuration Guide*.

   ONTAP Configuration Guide

7. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

b. Register your system.

NetApp Product Registration

c. Download Active IQ Config Advisor.

NetApp Downloads: Config Advisor

8. Verify the health of your system by running Config Advisor.
9. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

**Option 2: Completing system setup and configuration if network discovery is not enabled**

If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

**Steps**

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

   See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console using the console cable that came with your system, and then connect the laptop to the management switch on the management subnet .
   c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.
2. Use the following animation to set one or more drive shelf IDs:

   Setting drive shelf IDs

3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.

   FAS8300 and FAS8700 shown.

   Power on the controllers

   Initial booting may take up to eight minutes.

4. Assign an initial node management IP address to one of the nodes.

| If the management network has DHCP… | Then… |
|---|---|
| Configured | Record the IP address assigned to the new controllers. |

| If the management network has DHCP… | Then… |
| --- | --- |
| Not configured | a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment.<br>Check your laptop or console's online help if you do not know how to configure PuTTY.<br>b. Enter the management IP address when prompted by the script. |

5. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

      The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the *NetApp ONTAP Configuration guide*.

      ONTAP Configuration Guide

6. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

   b. Register your system.

      NetApp Product Registration

   c. Download Active IQ Config Advisor.

      NetApp Downloads: Config Advisor

7. Verify the health of your system by running Config Advisor.
8. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

## Maintain

### Boot media

#### Overview of boot media replacement - AFF FAS8300 and FAS8700

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` file.

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 must be connected to a network to restore the `var` file system.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct node:
  - The *impaired* node is the node on which you are performing maintenance.
  - The *healthy node* is the HA partner of the impaired node.

#### Check onboard encryption keys - AFF fas8300 and FAS8700

## Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

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 the NetApp Encryption overview with the CLI.

**Steps**

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. 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`
3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to the next section.
4. If the impaired controller is part of an HA configuration, disable automatic giveback from the healthy controller: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

#### Check NVE or NSE on systems running ONTAP 9.6 and later

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

#### Verify NVE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`
     e. Shut down the impaired controller.
  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

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.

   mysupport.netapp.com

b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

   > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

### Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     d. Return to admin mode: `set -priv admin`
     e. You can safely shut down the controller.
  2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
     a. Enter the onboard security key-manager sync command: `security key-manager external sync`

        If the command fails, contact NetApp Support.

        mysupport.netapp.com

     b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
     c. You can safely shut down the controller.
  3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
     a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

        Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

        mysupport.netapp.com

     b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
     c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
     d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`
     f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
     g. Return to admin mode: `set -priv admin`
     h. You can safely shut down the controller.

### 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 `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name`<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

1. 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 controller.

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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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 controller.

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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |

| If the impaired controller… | Then… |
| --- | --- |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

#### Replace the boot media - FAS8300 and FAS8700

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 module

To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

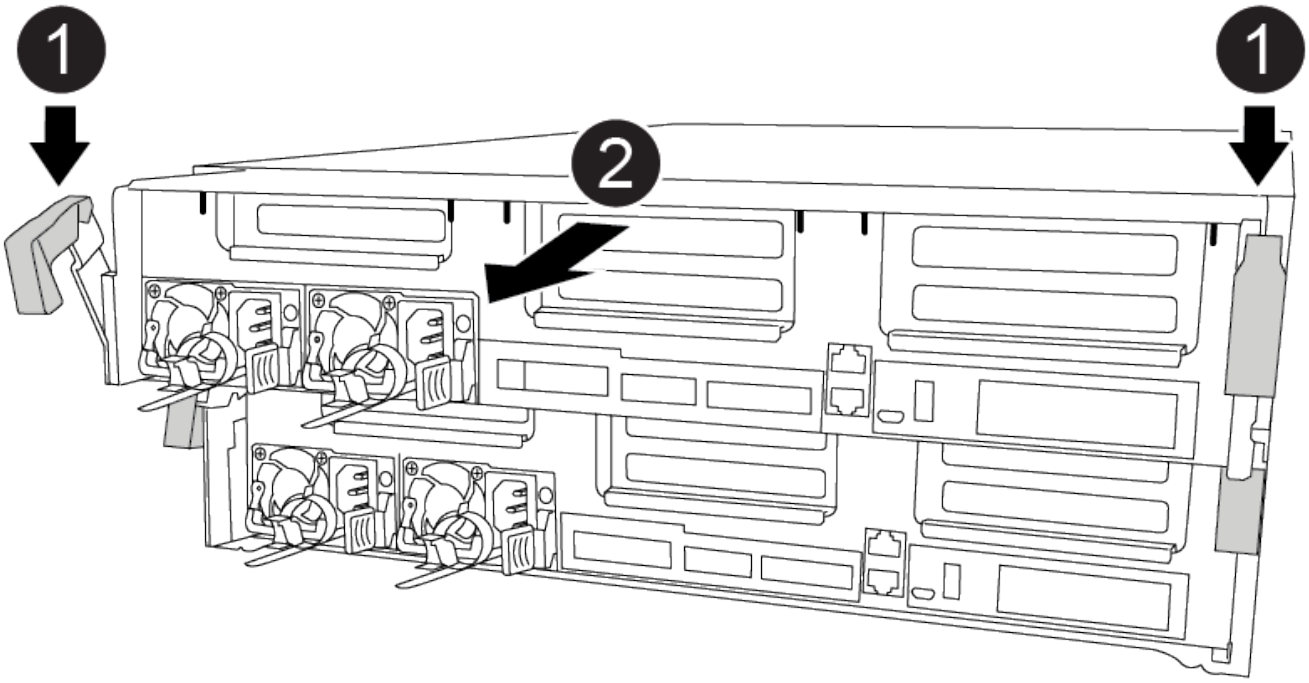
#### Steps

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.



| | |
|---|---|
| 1 | Locking latches |
| 2 | Slide controller out of chassis |

6. 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.

7. Place the controller module on a stable, flat surface.

### Step 2: Replace the boot media

## You must locate the boot media in the controller module (see the FRU map on the controller module), and then follow the directions to replace it.

#### Before you begin

Although the contents of the boot media is encrypted, it is a best practice to erase the contents of the boot media before replacing it. For more information, see the Statement of Volatility for your system on the NetApp Support Site.

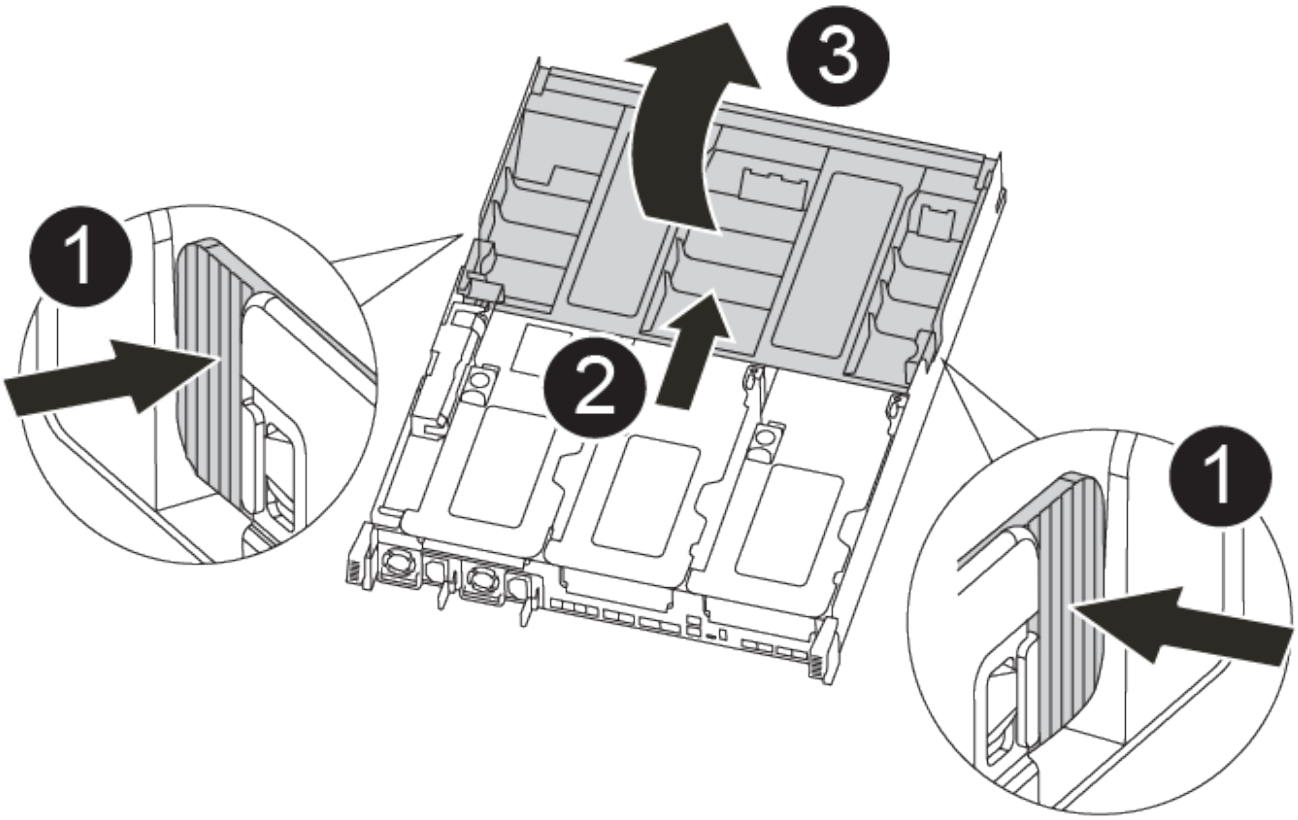
> You must log into the NetApp Support Site to display the *Statement of Volatility* for your system.

You can use the following animation, illustrations, or the written steps to replace the boot media.

Replacing the boot media

#### Steps

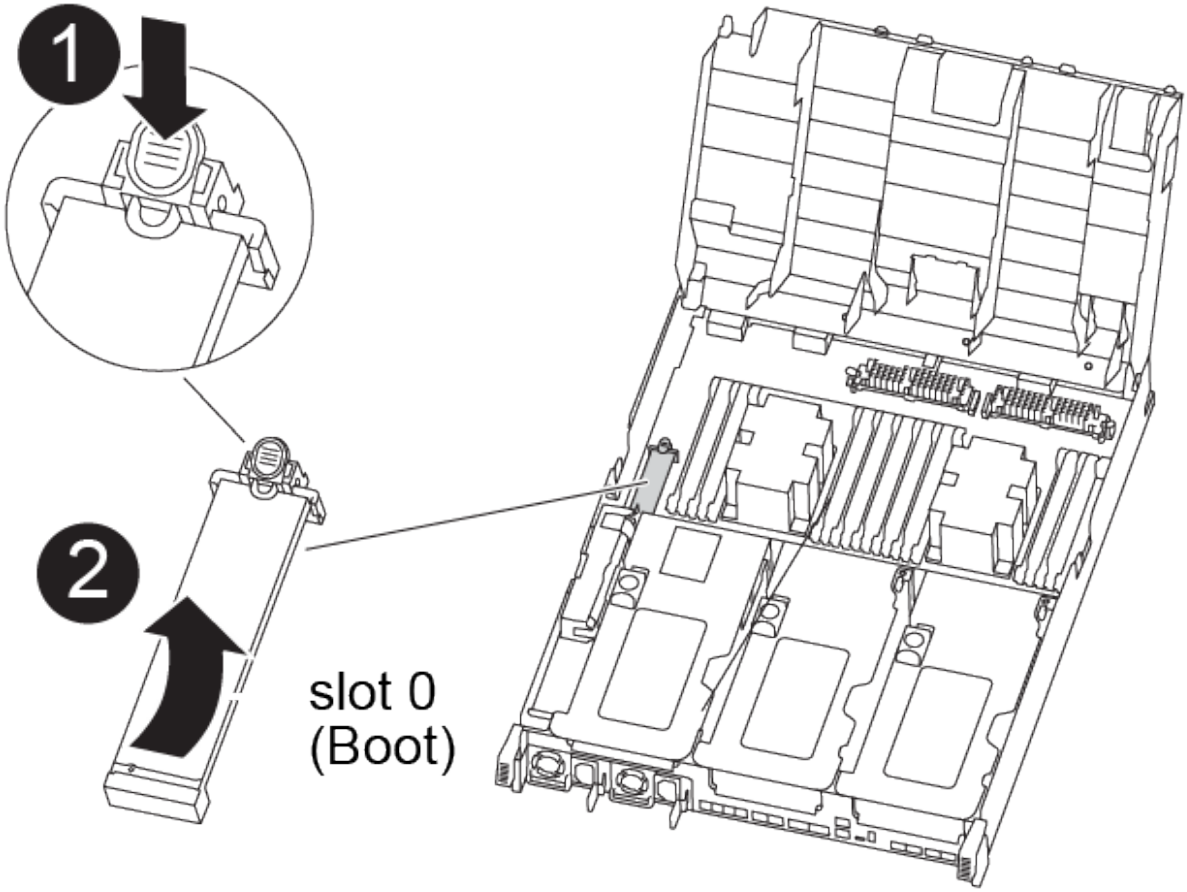
1. Open the air duct:




| | |
|---|---|
| 1 | Locking tabs |
| 2 | Slide air duct toward back of controller |
| 3 | Rotate air duct up |

a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.

2. Locate and remove the boot media from the controller module:




| | |
|---|---|
| 1 | Press blue button |
| 2 | Rotate boot media up and remove from socket |

a. Press the blue button at the end of the boot media until the lip on the boot media clears the blue button.
b. Rotate the boot media up and gently pull the boot media out of the socket.

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

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

5. Lock the boot media in place:
   a. Rotate the boot media down toward the motherboard.
   b. Placing a finger at the end of the boot media by the blue button, push down on the boot media end to engage the blue locking button.
   c. While pushing down on the boot media, lift the blue locking button to lock the boot media in place.
6. Close the air duct.

#### Step 3: Transfer the boot image to the boot media

The replacement boot media that you installed does not have a boot image, so you need to transfer a boot image using a USB flash drive.

**Before you begin**

- You must have a USB flash drive, formatted to MBR/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 an HA pair, you must have a network connection.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the `var` file system.

1. Download and copy the appropriate service image from the NetApp Support Site to the USB flash drive.
   a. Download the service image to your work space on your laptop.
   b. Unzip the service image.

      > If you are extracting the contents using Windows, do not use WinZip to extract the netboot image. Use another extraction tool, such as 7-Zip or WinRAR.

      There are two folders in the unzipped service image file:

      - `boot`
      - `efi`

   c. Copy the `efi` folder to the top directory on the USB flash drive.

      The USB flash drive should have the efi folder and the same Service Image (BIOS) version of what the impaired controller is running.

   d. Remove the USB flash drive from your laptop.
2. If you have not already done so, close the air duct.
3. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
4. Reinstall the cable management device and recable the system, as needed.

   When recabling, remember to reinstall the media converters (SFPs or QSFPs) if they were removed.
5. Plug the power cable into the power supply and reinstall the power cable retainer.
6. 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.

7. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   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. If you have not already done so, reinstall the cable management device.
8. Interrupt the boot process by pressing Ctrl-C to stop at the LOADER prompt.

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

9. 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 FAS8300 and FAS8700

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

**Option 1: 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 | a. Press `y` when prompted to restore the backup configuration.<br>b. Set the healthy controller to advanced privilege level: `set -privilege advanced`<br>c. Run the restore backup command: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`*<br>d. Return the controller to admin level: `set -privilege admin`<br>e. Press `y` when prompted to use the restored configuration.<br>f. Press `y` when prompted to reboot the controller. |
| No network connection | a. Press `n` when prompted to restore the backup configuration.<br>b. Reboot the system when prompted by the system.<br>c. Select the **Update flash from backup config** (sync flash) option from the displayed menu.<br>If you are prompted to continue with the update, press `y`. |

4. Ensure that the environmental variables are set as expected:
   a. Take the controller 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 controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

7. Connect the console cable to the partner controller.
8. Give back the controller 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 controller 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: Controller is in a two-node MetroCluster**

## 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 fas8300 and FAS8700

## After you have completed the FRU replacement in a two-node MetroCluster configuration, you can perform the MetroCluster switchback operation. This returns the

configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the formerly impaired site now active and serving data from the local disk pools.

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 OKM, NSE, and NVE as needed - AFF fas8300 and FAS8700

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

1. Determine which section you should use to restore your OKM, NSE, or NVE configurations: If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.
   - If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Restore NVE or NSE when Onboard Key Manager is enabled.
   - If NSE or NVE are enabled for ONTAP 9.6, go to Restore NSE/NVE on systems running ONTAP 9.6 and later.

#### Restore NVE or NSE when Onboard Key Manager is enabled

**Steps**

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
|---|---|
| The LOADER prompt | Boot the controller to the boot menu: `boot_ontap menu` |
| Waiting for giveback…. | a. Enter `Ctrl-C` at the prompt<br>b. At the message: Do you wish to halt this node rather than wait [y/n]? , enter: `y`<br>c. At the LOADER prompt, enter the `boot_ontap menu` command. |

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.

6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command

> The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

Example of backup data:


```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to Waiting for giveback… prompt.

8. Move the console cable to the partner controller and login as "admin".
9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Giveback only the CFO aggregates with the `storage failover giveback -fromnode local -only-cfo-aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

      > Terminating CIFS can cause loss of data.

    - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show`

and `storage failover show-giveback` commands.

Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. Move the console cable to the target controller.
    a. If you are running ONTAP 9.6 or later, run the security key-manager onboard sync:
    b. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    c. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    d. Wait 10 minutes for the key to synchronize across the cluster.
13. Move the console cable to the partner controller.
14. Give back the target controller using the `storage failover giveback -fromnode local` command.
15. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

16. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

17. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
18. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

### Restore NSE/NVE on systems running ONTAP 9.6 and later

#### Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
| --- | --- |
| The login prompt | Go to Step 7. |

| | |
|---|---|
| Waiting for giveback… | a. Log into the partner controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

    - If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

      Use the `security key-manager key query` command to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

#### Return the failed part to NetApp - AFF fas8300 and FAS8700

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Replace the caching module - FAS8300 and FAS8700

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation.

- 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 tasks**

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.

ONTAP 9 System Administration Reference

You might want to erase the contents of your caching module before replacing it.

**Steps**

1. Although data on the caching module is encrypted, you might want to erase any data from the impaired caching module and verify that the caching module has no data:

   a. Erase the data on the caching module: `system controller flash-cache secure-erase run -node node_name -device-id device_id`

   b. Verify that the data has been erased from the caching module: `system controller flash-cache secure-erase show -node node_name`

      The output should display the caching module status as erased.

2. 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_down_h`

   The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

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

4. 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 `y`. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller: `storage failover takeover -ofnode impaired_node_name` When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

**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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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: -
```

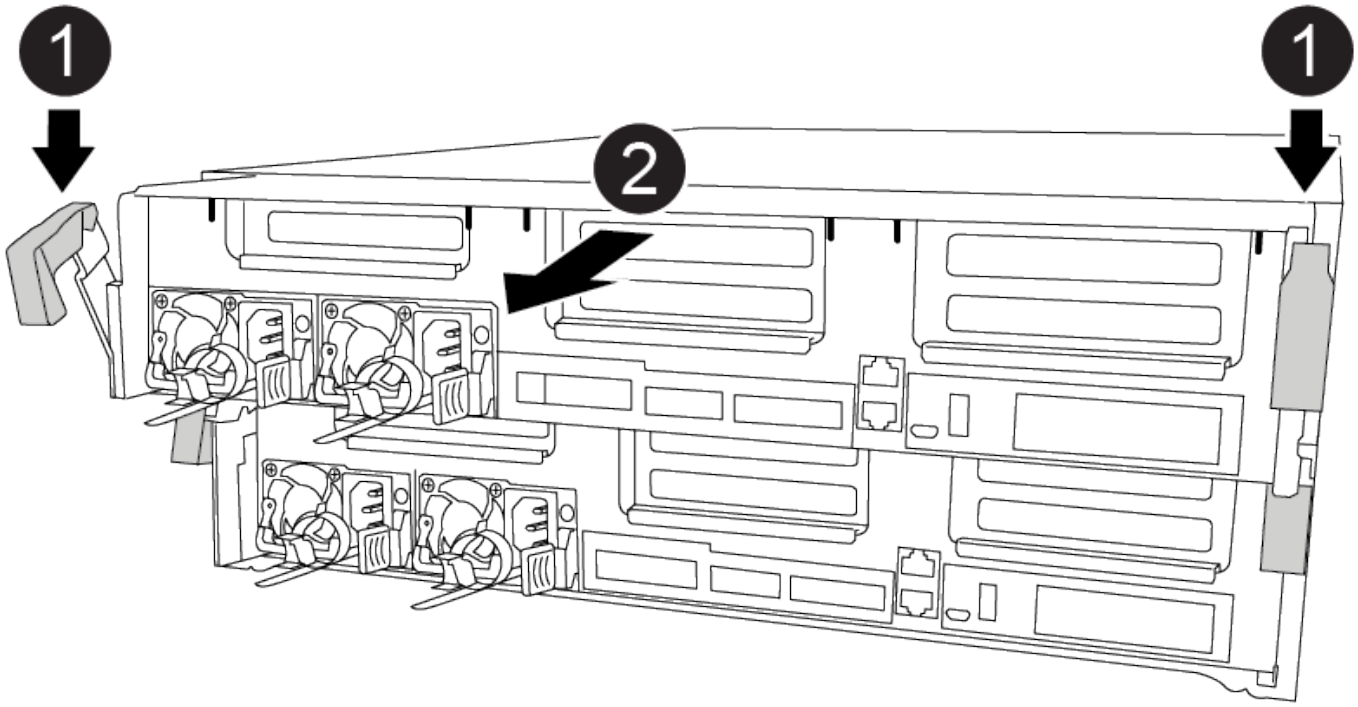
8. On the impaired controller module, disconnect the power supplies.

**Step 2: Remove the controller module**

## To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module




**Steps**

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. 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.

7. Place the controller module on a stable, flat surface.

#### Step 3: Replace a caching module

To replace a caching module, referred to as the Flash Cache on the label on your controller, locate the slot inside the controller and follow the specific sequence of steps. See the FRU map on the controller module for the location of the Flash Cache.

Your storage system must meet certain criteria depending on your situation:

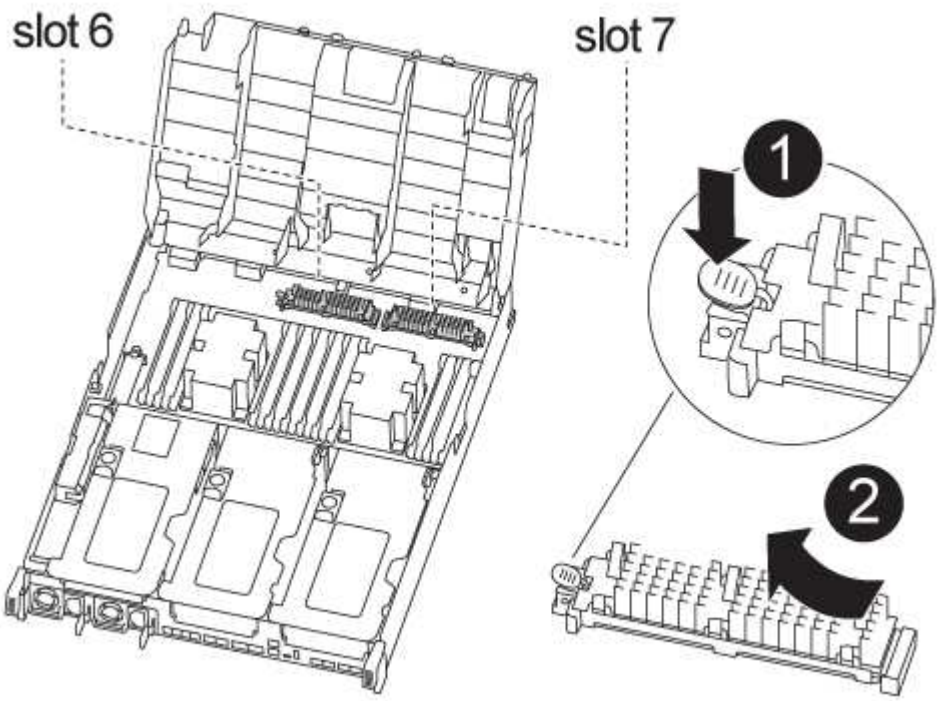
- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- Although the contents of the caching module is encrypted, it is a best practice to erase the contents of the module before replacing it. For more information, see the Statement of Volatility for your system on the NetApp Support Site.

> You must log into the NetApp Support Site to display the *Statement of Volatility* for your system.

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

You can use the following animation, illustration, or the written steps to replace a caching module.

Replacing the caching module




**Steps**

1. If you are not already grounded, properly ground yourself.
2. Open the air duct:
   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.

b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.

3. Using the FRU map on the controller module, locate the failed caching module and remove it:

   Depending on your configuration, there may be zero, one, or two caching modules in the controller module. The failed caching module's LED is lit.

   a. Press the blue release tab.

      The caching module end rises clear of the release tab.

   b. Rotate the caching module up and slide it out of the socket.

4. Install the replacement caching module:
   a. Align the edges of the replacement caching module with the socket and gently insert it into the socket.
   b. Rotate the caching module downward toward the motherboard.
   c. Placing your finger at the end of the caching module by the blue button, firmly push down on the caching module end, and then lift the locking button to lock the caching module in place.

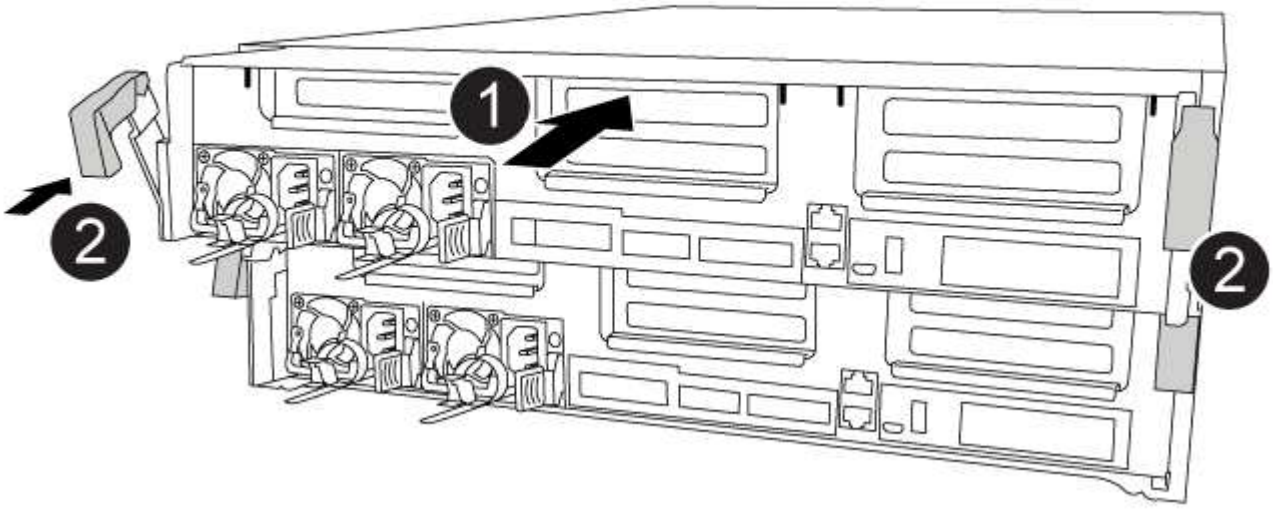
5. Close the air duct:
   a. Rotate the air duct down to the controller module.
   b. Slide the air duct toward the risers to lock it in place.

#### Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module



**Steps**

1. If you have not already done so, close the air duct.
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. 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.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

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

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

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

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      > If your system stops at the boot menu, select the option to boot to LOADER.

   f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.
   g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

      If your system stops at the boot menu, select the option to boot to LOADER.

#### Step 5: Run diagnostics

## After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

**Steps**

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Stress-Test system** from the displayed menu.
5. Select **M.2 NVME Drive Stress** from the displayed menu.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

#### Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

**Steps**

1. 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.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

#### Step 7: Switch back aggregates in a two-node MetroCluster configuration

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

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 8: Complete the replacement process

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Chassis

#### Overview of chassis replacement - FAS8300 and FAS8700

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-controller cluster, you will have a complete service outage and a partial outage in a multi-node cluster.

#### Shut down the controllers - FAS8300 and FAS8700

### Option 1: Most configurations

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

#### About this task

- If you have a cluster with more than two controllers, 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 the Administration overview with the CLI.
- 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`

#### Steps

1. If your system has two controller modules, disable the HA pair.

| If your system is running clustered ONTAP with… | Then… |
|---|---|
| Two controllers in the cluster | `cluster ha modify -configured false` `storage failover modify -node node0 -enabled false` |
| More than two controllers in the cluster | `storage failover modify -node node0 -enabled false` |

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

> You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

#### Option 2: Controller is 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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |

| If the impaired controller… | Then… |
| --- | --- |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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 - FAS8300 and FAS8700

## 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 controller modules

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

#### Steps

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove and set aside the cable management devices from the left and right sides of the controller module.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. 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.

7. Set the controller module aside in a safe place, and repeat these steps for the other controller module in the chassis.

### Step 2: Move the fans

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

#### 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. Press down the release latch on the fan module cam handle, and then rotate the cam handle downward.

   The fan module moves a little bit away from the chassis.

4. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

   > 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.

5. Set the fan module aside.
6. Repeat the preceding steps for any remaining fan modules.
7. Insert the fan module into the replacement chassis by aligning it with the opening, and then sliding it into the chassis.
8. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

   The cam handle raises slightly when the fan module is completely seated.

9. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The fan LED should be green after the fan is seated and has spun up to operational speed.

10. Repeat these steps for the remaining fan modules.

### Step 3: Replace a chassis from within the equipment rack or system cabinet

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

#### Steps

1. Remove the screws from the chassis mount points.
2. With two people, slide the old chassis off the rack rails in a system cabinet or equipment rack, and then set it aside.
3. If you are not already grounded, properly ground yourself.
4. Using two 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 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. If you have not already done so, install the bezel.

### Step 4: Install the controller modules

After you install the controller modules into the new chassis, you need to boot it to a state where you can run the diagnostic test.

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. 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. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

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

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

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

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      > If your system stops at the boot menu, select the option to boot to LOADER.

   f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.
   g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

      If your system stops at the boot menu, select the option to boot to LOADER.

4. Repeat the preceding steps to install the second controller into the new chassis.

#### Complete the restoration and replacement process - FAS8300 and FAS8700

You must verify the HA state of the chassis, run diagnostics, 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.

### Step 2: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

#### Steps

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test system** from the displayed menu to run diagnostics tests.
5. Select the test or series of tests from the various sub-menus.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select Reboot from the menu to reboot the system.

### Step 3: Switch back aggregates in a two-node MetroCluster configuration

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

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: Complete the replacement process

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Controller

#### Overview of controller module replacement - FAS8300 and FAS8700

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 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 controller 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 controller to the *replacement* controller so that the *replacement* controller 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* controller is the controller that is being replaced.
  - The *replacement node* is the new controller that is replacing the impaired controller.
  - The *healthy* controller is the surviving controller.
- You must always capture the controller'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 - FAS8300 and FAS8700

You can shut down or take over the impaired controller using different procedures, depending on the storage system hardware 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 are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Returning SEDs to unprotected mode" section of the *ONTAP 9 NetApp Encryption Power Guide*.

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

#### Replace the controller module hardware - FAS8300 and FAS8700

## To replace the controller module hardware, you must remove the impaired controller, 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 module, you must remove the controller module from the chassis.

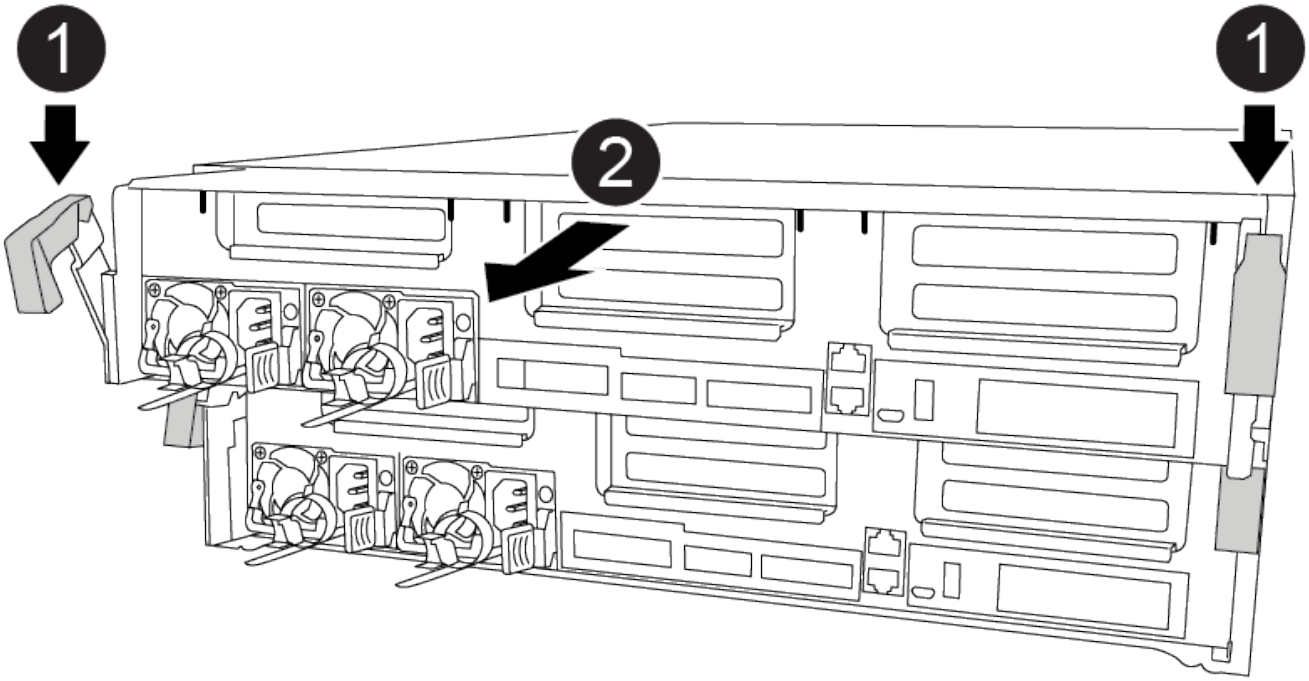
You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.



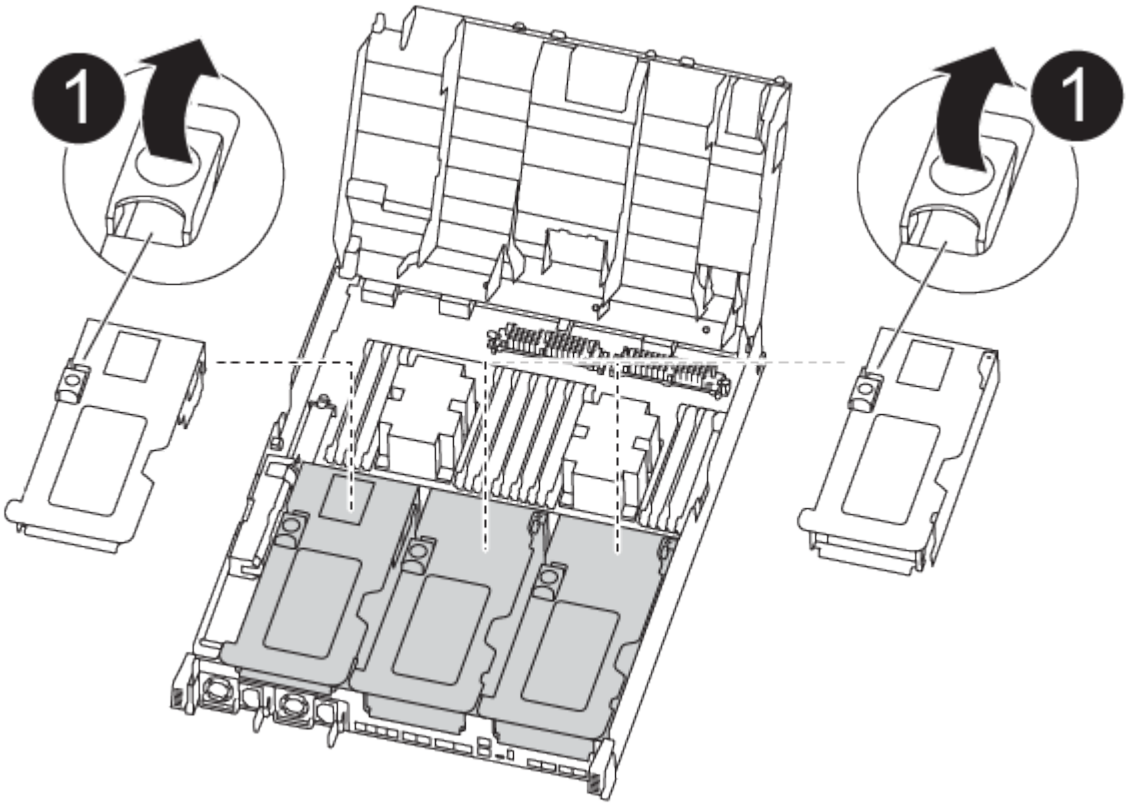

   The controller module moves slightly out of the chassis.

6. 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.

7. Place the controller module on a stable, flat surface.
8. On the replacement controller module, open the air duct and remove the empty risers from the controller module using the animation, illustration, or the written steps:

   Removing the empty risers from the replacement controller module



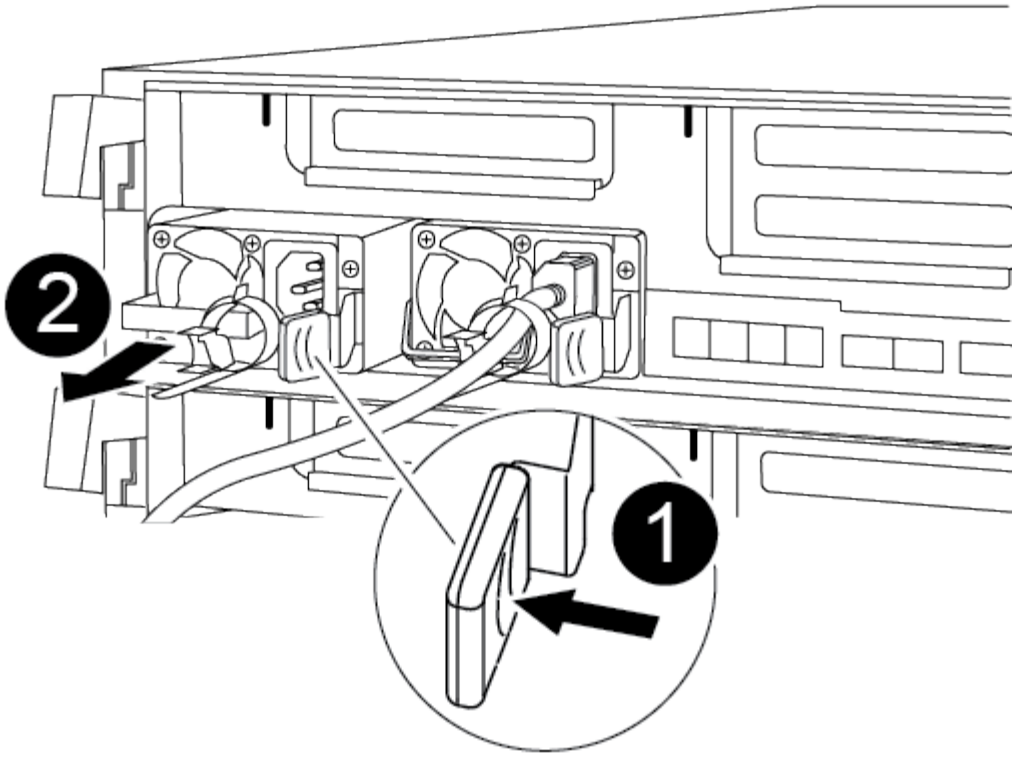

a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
c. Rotate the riser locking latch on the left side of riser 1 up and toward air duct, lift the riser up, and then set it aside.
d. Repeat the previous step for the remaining risers.

**Step 2: Move the power supplies**

You must move the power supply from the impaired controller module to the replacement controller module when you replace a controller module.

You can use the following animation, illustration, or the written steps to move the power supplies to the replacement controller module.

Moving the power supplies




1. Remove the power supply:
   a. Rotate the cam handle so that it can be used to pull the power supply out of the chassis.
   b. Press the blue locking tab to release the power supply from the chassis.
   c. Using both hands, pull the power supply out of the chassis, and then set it aside.
2. Move the power supply to the new controller module, and then install it.
3. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

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

**Step 3: Move the NVDIMM battery**

To move the NVDIMM battery from the impaired controller module to the replacement controller module, you must perform a specific sequence of steps.

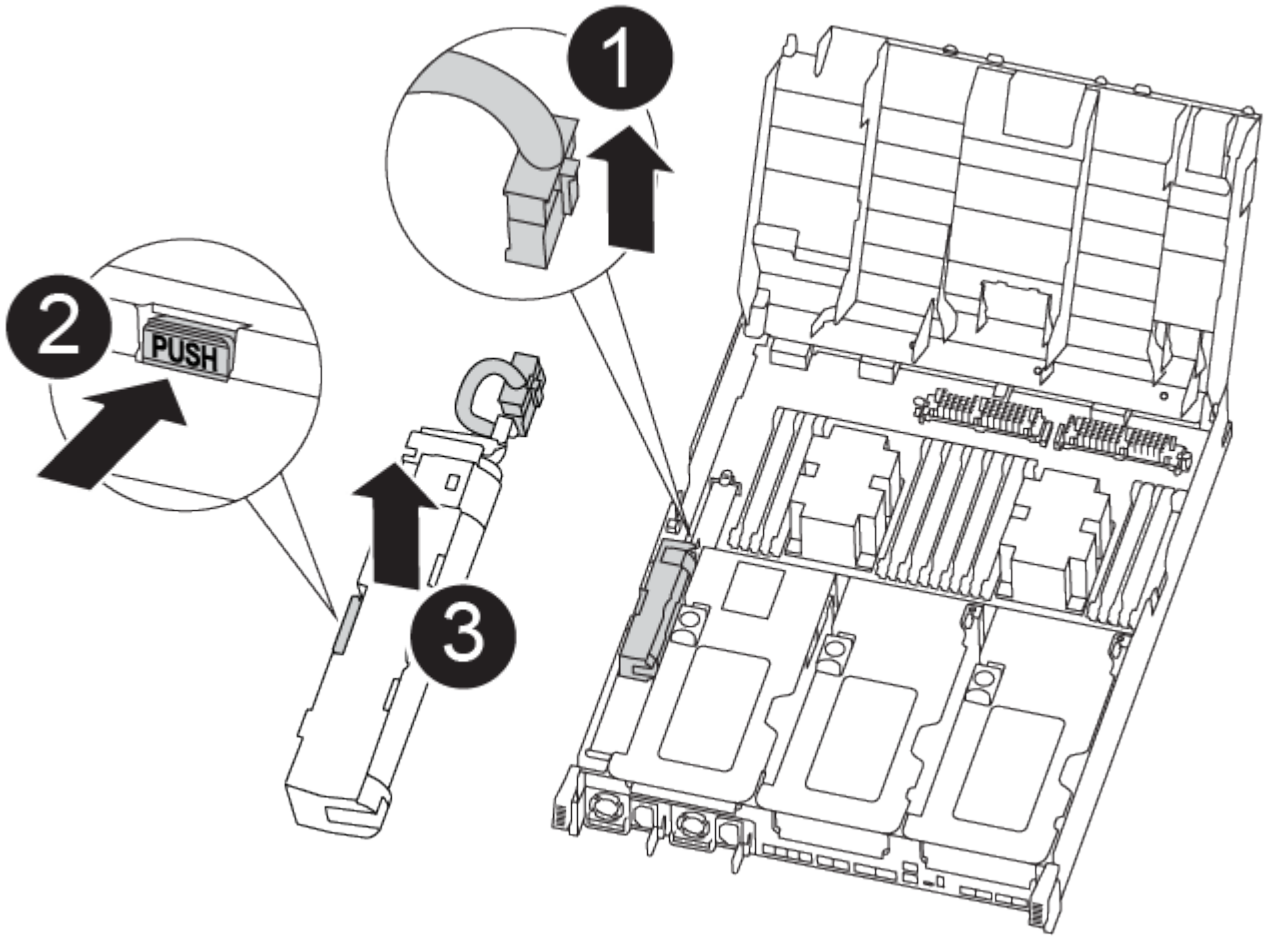
You can use the following animation, illustration, or the written steps to move the NVDIMM battery from the impaired controller module to the replacement controller module.

Moving the NVDIMM battery

1. Open the air duct:

a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.

2. Locate the NVDIMM battery in the controller module.




1. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket, and then unplug the battery cable from the socket.
2. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
3. Move the battery to the replacement controller module.
4. Align the battery module with the opening for the battery, and then gently push the battery into slot until it locks into place.

> Do not plug the battery cable back into the motherboard until instructed to do so.

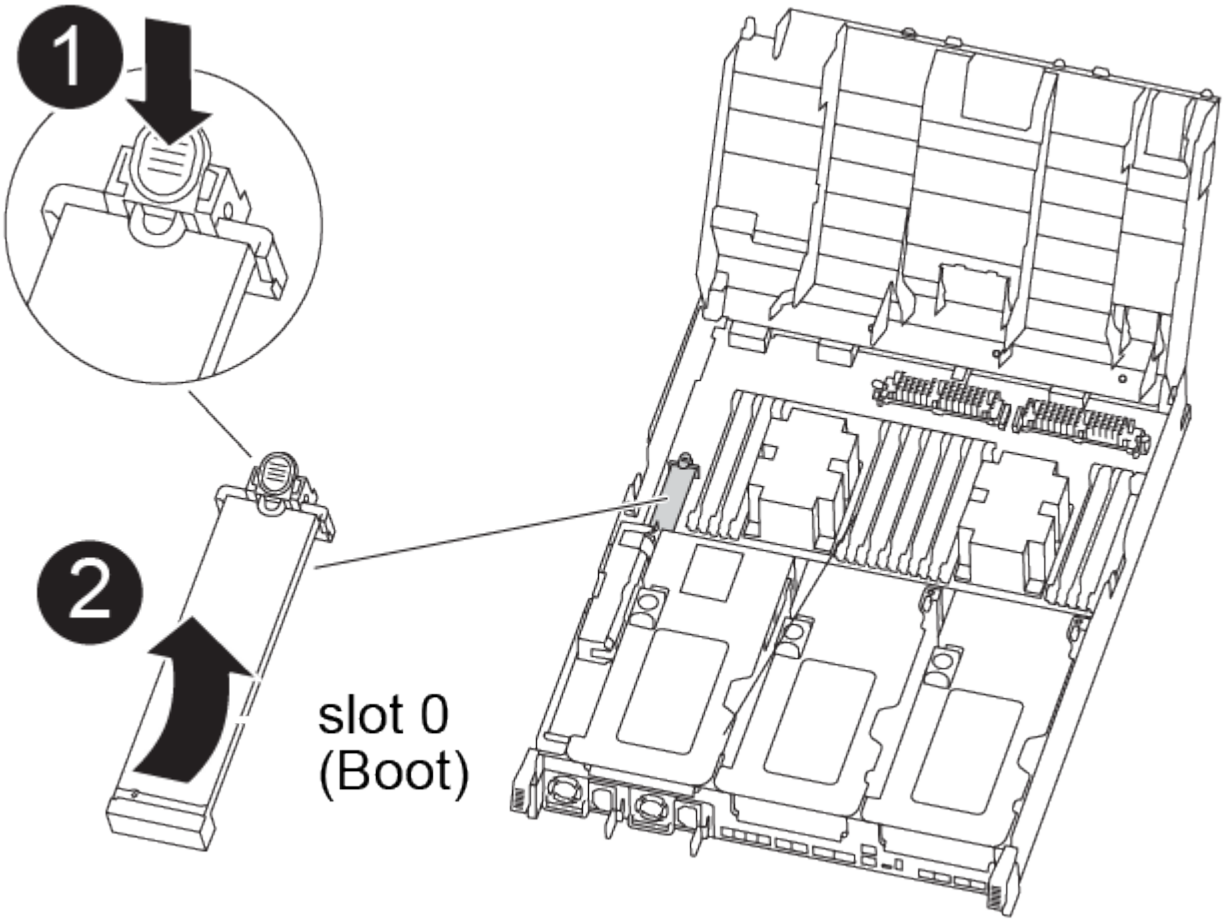
**Step 4: Move the boot media**

You must locate the boot media, and then follow the directions to remove it from the impaired controller module and insert it into the replacement controller module.

You can use the following animation, illustration, or the written steps to move the boot media from the impaired

controller module to the replacement controller module.

Moving the boot media




1. Locate and remove the boot media from the controller module:
   a. Press the blue button at the end of the boot media until the lip on the boot media clears the blue button.
   b. Rotate the boot media up and gently pull the boot media out of the socket.
2. 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.
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 reseat it into the socket.

4. Lock the boot media in place:
   a. Rotate the boot media down toward the motherboard.
   b. Press the blue locking button so that it is in the open position.
   c. Placing your fingers at the end of the boot media by the blue button, firmly push down on the boot media end to engage the blue locking button.

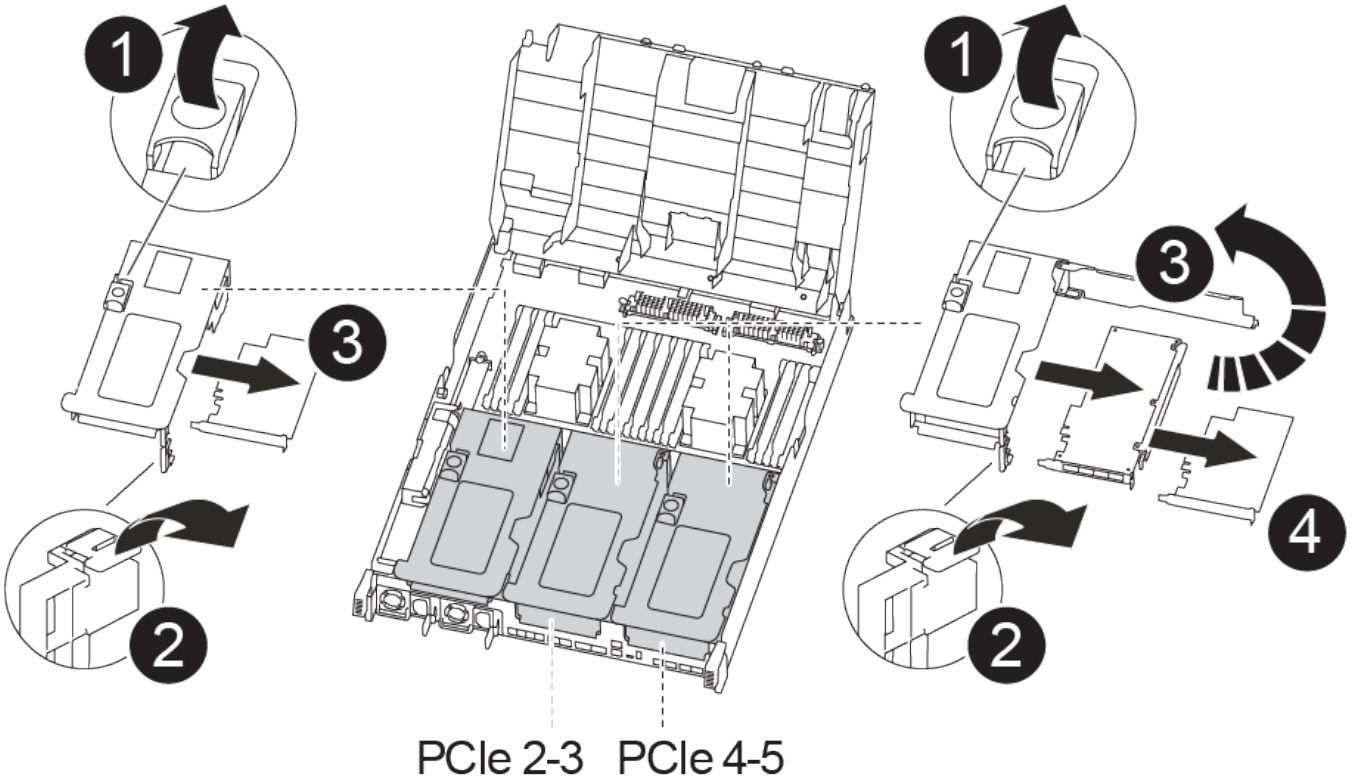
**Step 5: Move the PCIe risers and mezzanine card**

As part of the controller replacement process, you must move the PCIe risers and mezzanine card from the impaired controller module to the replacement controller module.

You can use the following animations, illustrations. or the written steps to move the PCIe risers and mezzanine card from the impaired controller module to the replacement controller module.

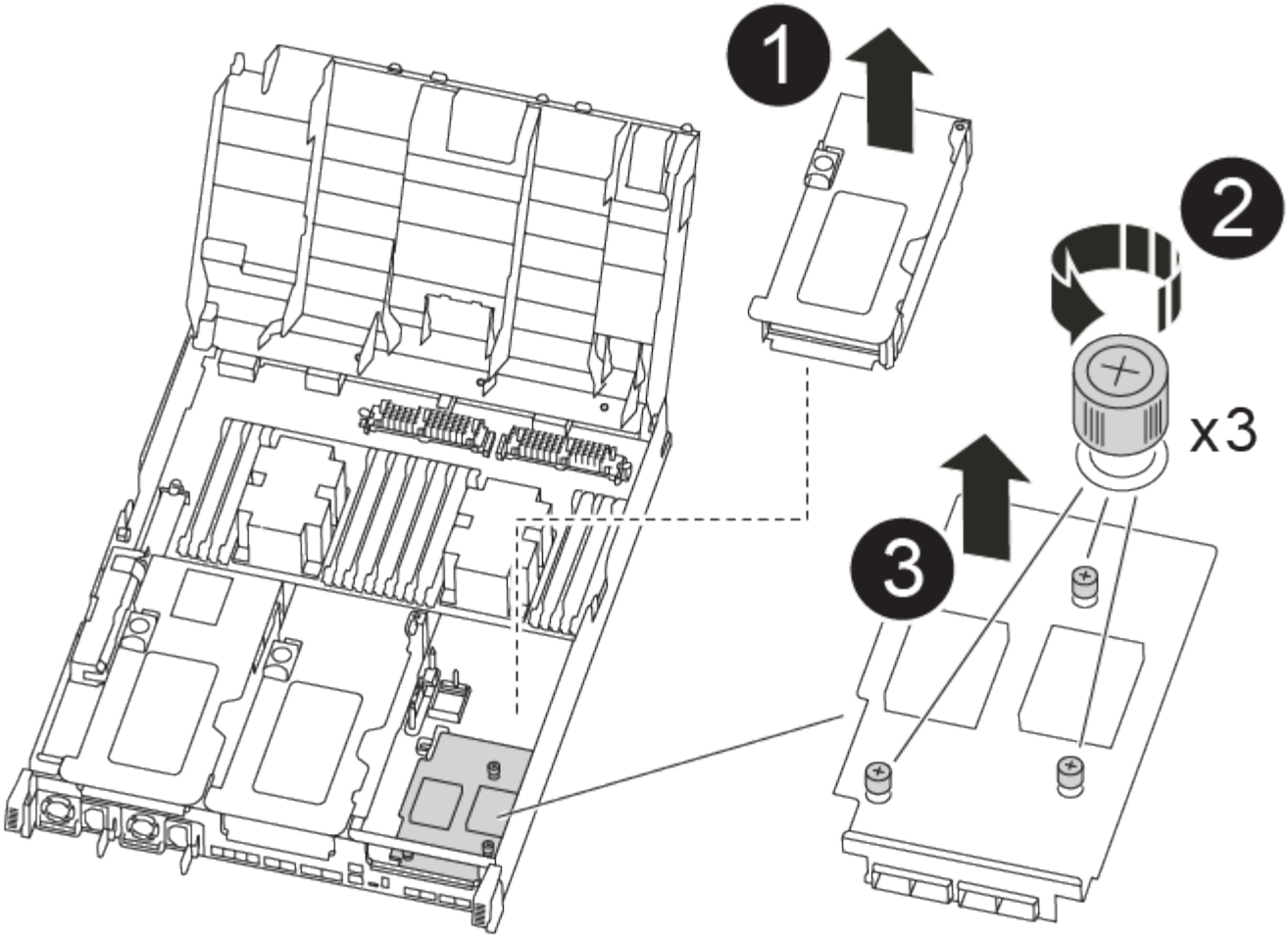
Moving PCIe riser 1 and 2 (left and middle risers):

Moving PCI risers 1 and 2




Moving the mezzanine card and riser 3 (right riser):

Moving the mezzanine card and riser 3




1. Move PCIe risers one and two from the impaired controller module to the replacement controller module:
   a. Remove any SFP or QSFP modules that might be in the PCIe cards.
   b. Rotate the riser locking latch on the left side of the riser up and toward air duct.

      The riser raises up slightly from the controller module.

   c. Lift the riser up, and then move it to the replacement controller module.
   d. Align the riser with the pins to the side of the riser socket, lower the riser down on the pins, push the riser squarely into the socket on the motherboard, and then rotate the latch down flush with the sheet metal on the riser.
   e. Repeat this step for riser number 2.
2. Remove riser number 3, remove the mezzanine card, and install both into the replacement controller module:
   a. Remove any SFP or QSFP modules that might be in the PCIe cards.
   b. Rotate the riser locking latch on the left side of the riser up and toward air duct.

      The riser raises up slightly from the controller module.

   c. Lift the riser up, and then set it aside on a stable, flat surface.
   d. Loosen the thumbscrews on the mezzanine card, and gently lift the card directly out of the socket, and then move it to the replacement controller module.

e. Install the mezzanine in the replacement controller and secure it with the thumbscrews.

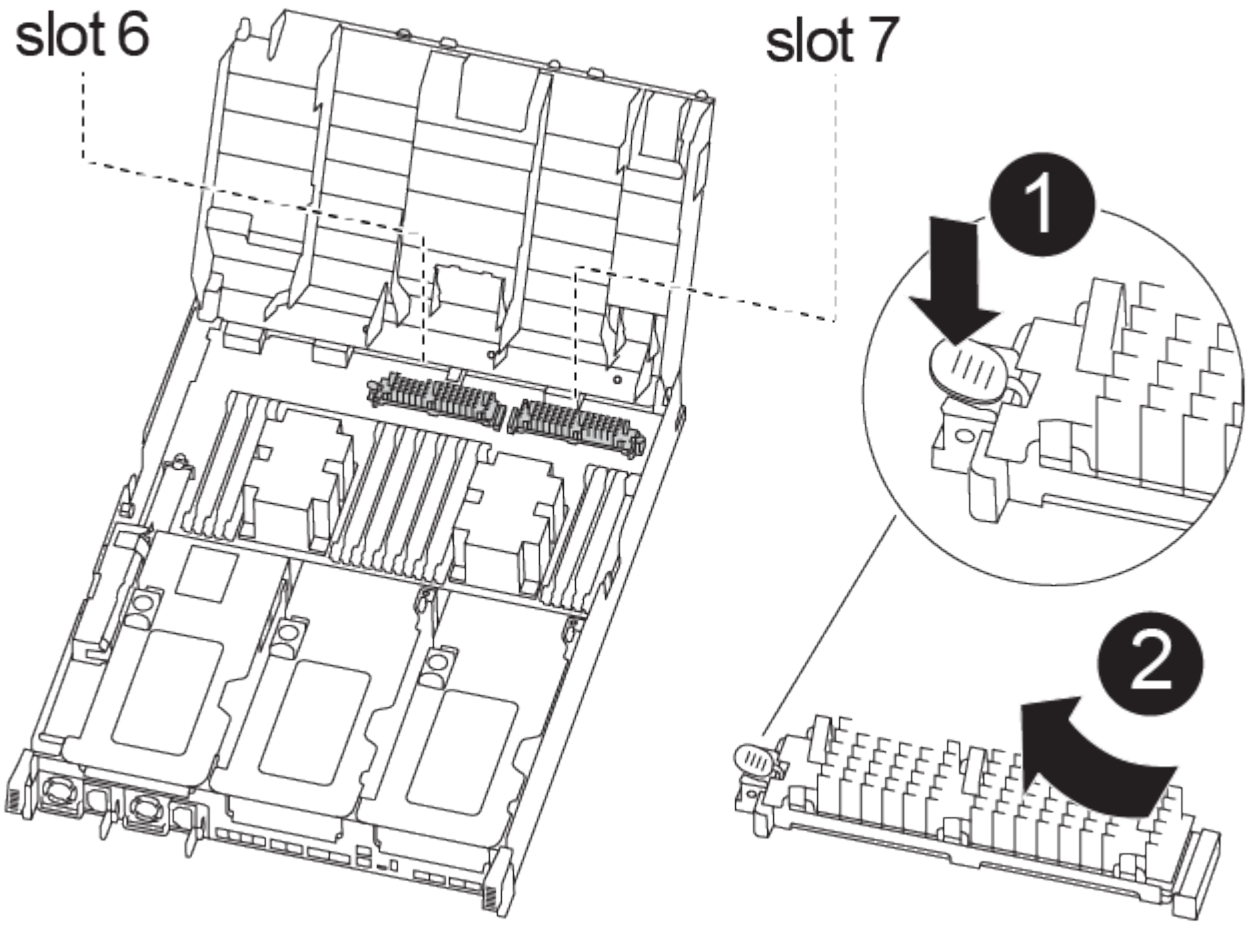
f. Install the third riser in the replacement controller module.

**Step 6: Move caching modules**

You must move the caching modules from the impaired controller modules to the replacement controller module when replacing a controller module.

You can use the following animation, illustration, or the written steps to move caching modules to the new controller module.

Moving the caching modules




1. If you are not already grounded, properly ground yourself.
2. Move the caching modules from the impaired controller module to the replacement controller module:
   a. Press the blue release tab at the end of the caching module, rotate the module up, and then remove the module from the socket.
   b. Move the caching module to the same socket on the replacement controller module.
   c. Align the edges of the caching module with the socket and gently insert the module as far into the socket as it will go.
   d. Rotate the caching module downward toward the motherboard.

e. Placing your finger at the end of the caching module by the blue button, firmly push down on the caching module end, and then lift the locking button to lock the caching module in place.

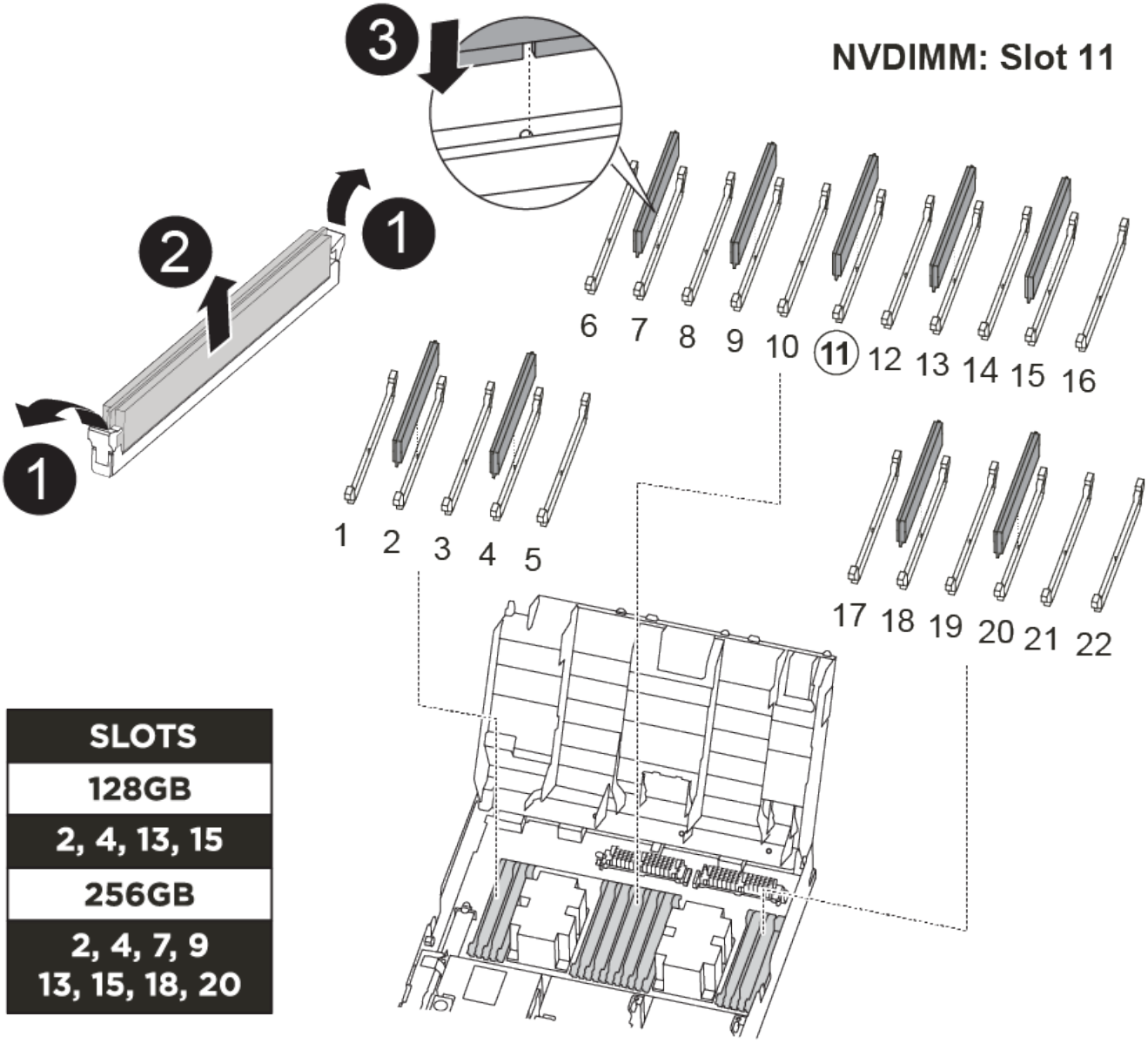
**Step 7: Move the DIMMs**

You need to locate the DIMMs, and then move them from the impaired controller module to the replacement controller module.

You must have the new controller module ready so that you can move the DIMMs directly from the impaired controller module to the corresponding slots in the replacement controller module.

You can use the following animation, illustration, or the written steps to move the DIMMs from the impaired controller module to the replacement controller module.

Moving the DIMMs




1. Locate the DIMMs on your controller module.

2. Note the orientation of the DIMM in the socket so that you can insert the DIMM in the replacement controller module in the proper orientation.
3. Verify that the NVDIMM battery is not plugged into the new controller module.
4. Move the DIMMs from the impaired controller module to the replacement controller module:

   > Make sure that you install the each DIMM into the same slot it occupied in the impaired controller module.

   a. Eject the DIMM from its slot by slowly pushing apart the 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.

   b. Locate the corresponding DIMM slot on the replacement controller module.
   c. Make sure that the DIMM ejector tabs on the DIMM socket are in the open position, and then insert the DIMM squarely into the socket.

      The DIMMs fit tightly in the socket, but should go in easily. If not, realign the DIMM with the socket and reinsert it.

   d. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.
   e. Repeat these substeps for the remaining DIMMs.
5. Plug the NVDIMM battery into the motherboard.

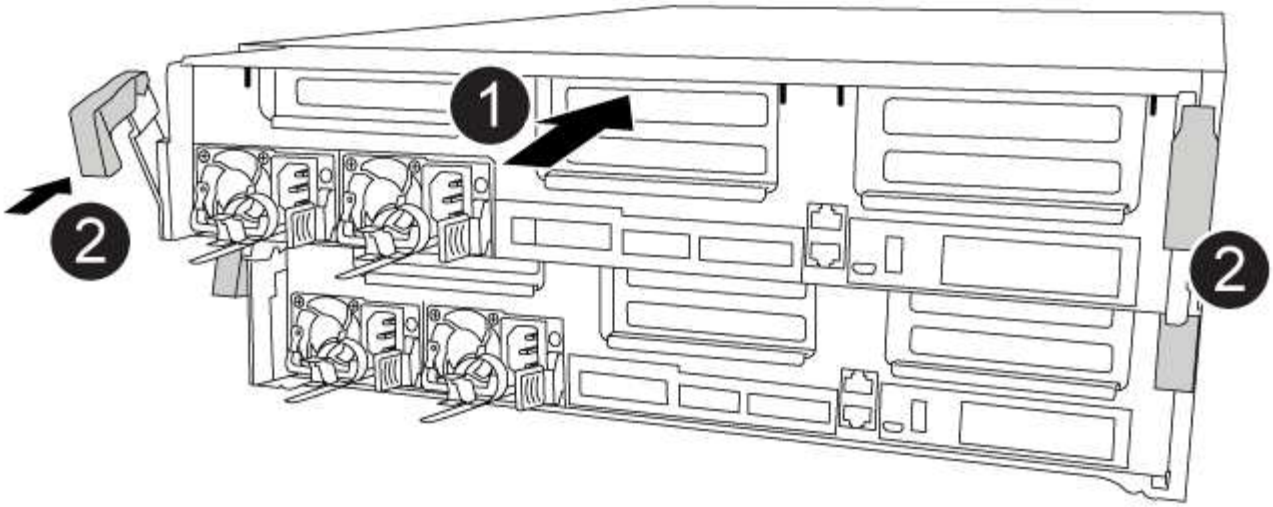
   Make sure that the plug locks down onto the controller module.

### Step 8: Install the controller module

After all of the components have been moved from the impaired controller module to the replacement controller module, you must install the replacement controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the replacement controller module in the chassis.

Installing the controller module




1. If you have not already done so, close the air duct.
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. 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.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

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

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

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

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.

g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

   If your system stops at the boot menu, select the option to boot to LOADER.

#### Restore and verify the system configuration - FAS8300 and FAS8700

## 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 after replacing the controller

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

#### About this task

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

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

#### Steps

1. 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: `show date`

   The date and time are given in GMT.

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 HA state of the controller module

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

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   The HA state should be the same for all components.

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

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

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

3. If the displayed system state of the controller module does not match your system configuration, set the `HA` state for the controller module: `ha-config modify controller ha-state`
4. Confirm that the setting has changed: `ha-config show`

**Step 3: Run diagnostics**

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node` *`node_name`*

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test system** from the displayed menu to run diagnostics tests.
5. Select the test or series of tests from the various sub-menus.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select `Reboot` from the menu to reboot the system.

     During the boot process, you might see the following prompts:

     - A prompt warning of a system ID mismatch and asking to override the system ID.
     - A prompt warning that when entering Maintenance mode in an HA configuration you must ensure that the healthy controller remains down.
       You can safely respond `y` to these prompts.

# You must complete a series of tasks before restoring your system to full operation.

## Step 1: Recable the system

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

### Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

## Step 2: Reassign disks

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

You must use the correct procedure for your configuration:

| Controller redundancy | Then use this procedure… |
|---|---|
| HA pair | Option 1: Verify the system ID change on an HA system] |
| Two-node MetroCluster configuration | Option 2: Manually reassign the system ID on systems in a two-node MetroCluster configuration |

## Option 1: Verify the system ID change on an HA system

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

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

1. If the *replacement* controller 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* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:
3. Wait until the `Waiting for giveback…` message is displayed on the *replacement* controller console and then, from the healthy controller, 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 controller, 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`
                                     Takeover
Node              Partner            Possible     State Description
------------      ------------       --------
-------------------------------------
node1             node2              false        System ID changed on
partner (Old:
                                                   151759755, New:
151759706), In takeover
node2             node1              -            Waiting for giveback
(HA mailboxes)
```

4. From the healthy controller, 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 controller:
   a. From the healthy controller, give back the replaced controller's storage: `storage failover giveback -ofnode` *`replacement_node_name`*

      The *replacement* controller 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* controller 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 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

#### Option 2: 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) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

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

   You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

   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   system-1  (118065481) Pool0  J8Y0TDZC       system-1
(118065481)
disk_name   system-1  (118065481) Pool0  J8Y09DXC       system-1
(118065481)
.
.
.
```

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

a. Change to the advanced privilege level: `set -privilege advanced`

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

b. Verify that the coredumps are saved: `system node run -node local-node-name partner savecore`

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

c. Return to the admin privilege level: `set -privilege admin`

7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
8. Boot the *replacement* node: `boot_ontap`
9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`
10. Verify the MetroCluster configuration: `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 - FAS8300 and FAS8700

To restore your system to full operation, you must restore the NetApp Storage Encryption configuration (if necessary), and install licenses for the new controller, and return the failed part to NetApp, as described in the RMA instructions shipped with the kit.

### Step 1: Install licenses for the replacement controller in ONTAP

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

#### About this task

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

#### Before you begin

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.

#### 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: Restore Storage and Volume Encryption functionality

After replacing the controller module or NVRAM module for a storage system that you previously configured to use Storage or Volume Encryption, you must perform additional steps to provide uninterrupted Encryption

functionality. You can skip this task on storage systems that do not have Storage or Volume Encryption enabled.

**Step**

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use 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

### Step 3: Verify LIFs and registering the serial number

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

**Steps**

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

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

2. Register the system serial number with NetApp Support.
   - 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. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

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

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

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 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 & Replacements page for further information.

### Replace a DIMM - FAS8300 and FAS8700

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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: -
```

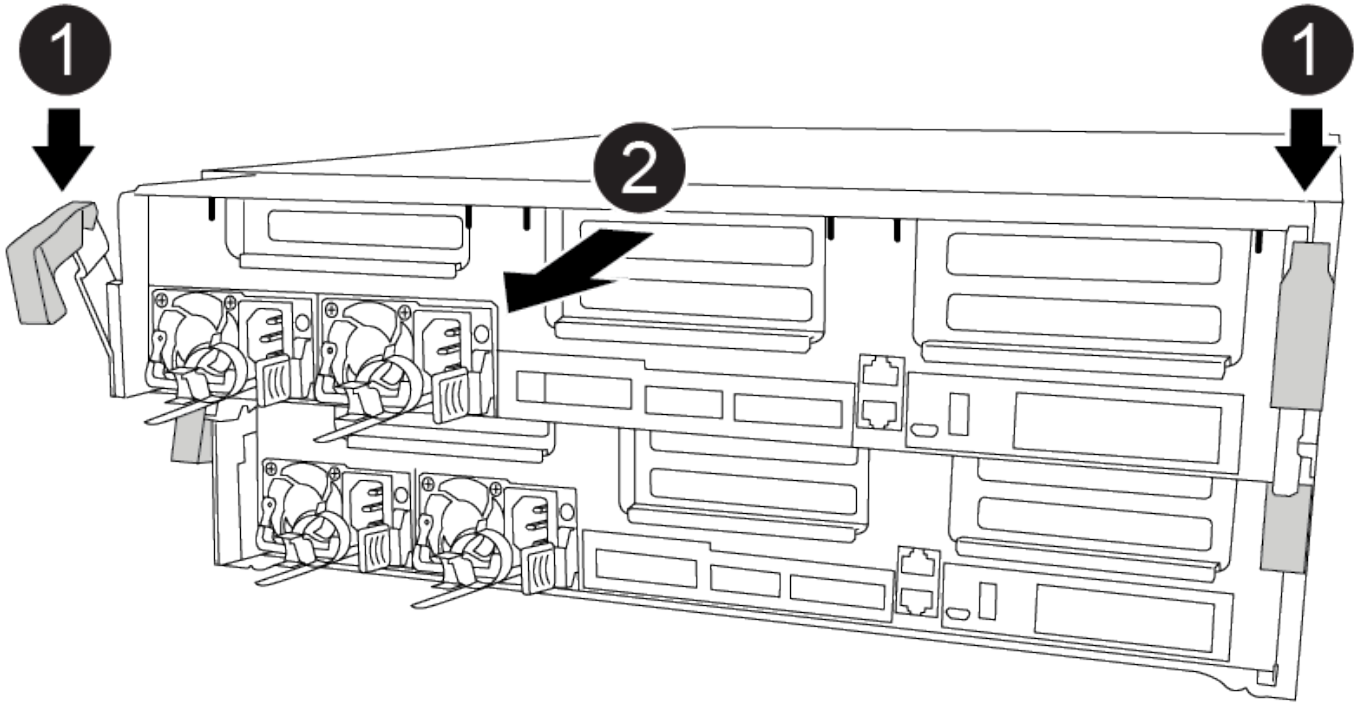
8. On the impaired controller module, disconnect the power supplies.

#### Step 2: Remove the controller module

## To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module




**Steps**

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. 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.

7. Place the controller module on a stable, flat surface.

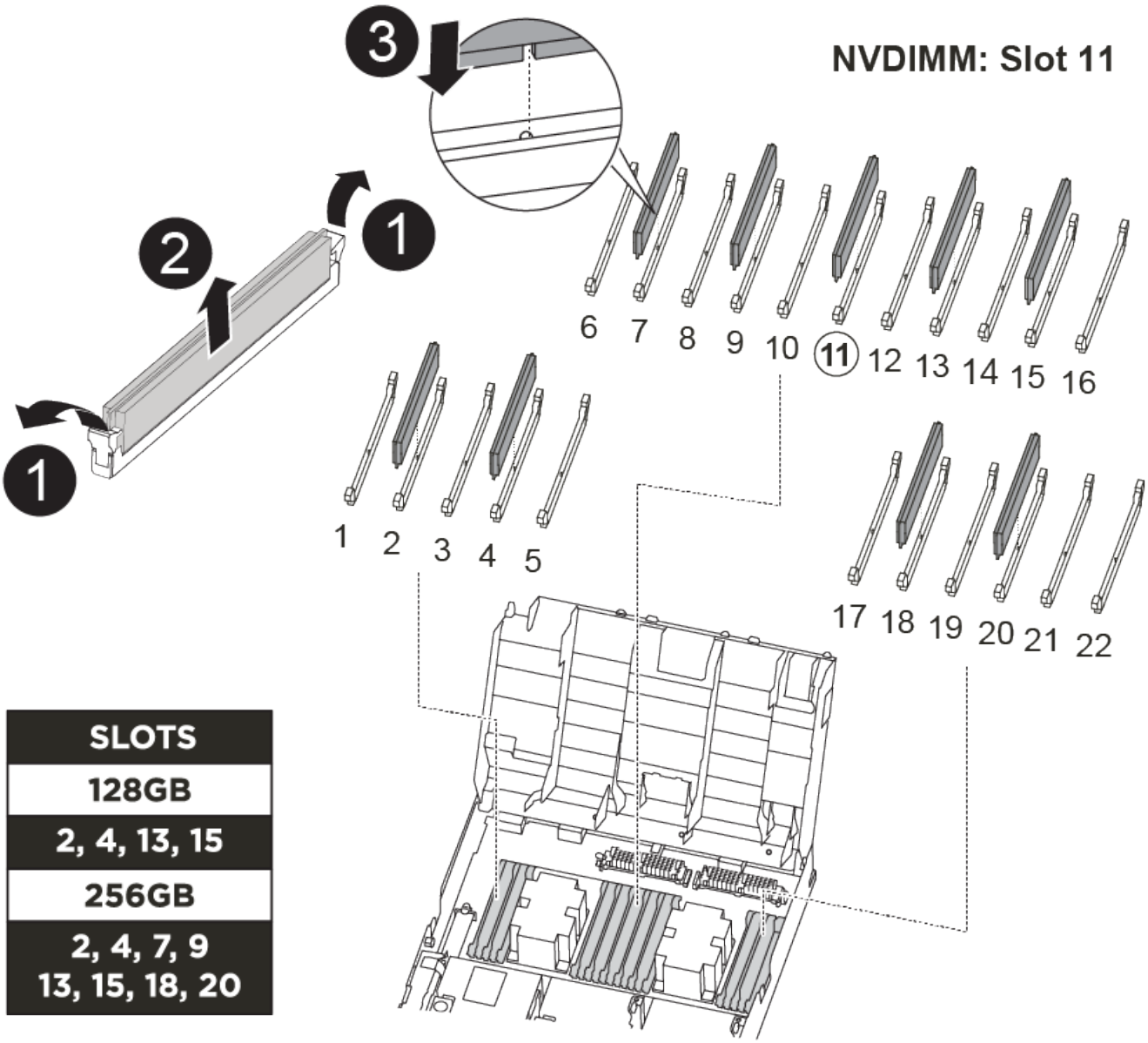
#### Step 3: Replace system DIMMs

Replacing a system DIMM involves identifying the target DIMM through the associated error message, locating the target DIMM using the FRU map on the air duct or the lit LED on the motherboard, and then replacing the DIMM.

You can use the following animation, illustration, or the written steps to replace a system DIMM.

> The animation and illustration shows empty slots for sockets without DIMMs. These empty sockets are populated with blanks.

Replacing a system DIMM




The number and location of DIMMS in your system depends on the model of your system. Refer to FRU map

on the air duct for more information.

- If you have a FAS8300 system, the system DIMMs are located in sockets 2, 4, 13, and 15.
- If you have a FAS8700 system, the system DIMMs are located in slots 2, 4, 7, 9, 13, 15, 18, and 20.
- The NVDIMM is located in slot 11.

**Steps**

1. Open the air duct:
   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
   b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
2. Locate the DIMMs on your controller module.
3. Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
4. Eject the DIMM from its socket by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the socket.

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

5. 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.

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.

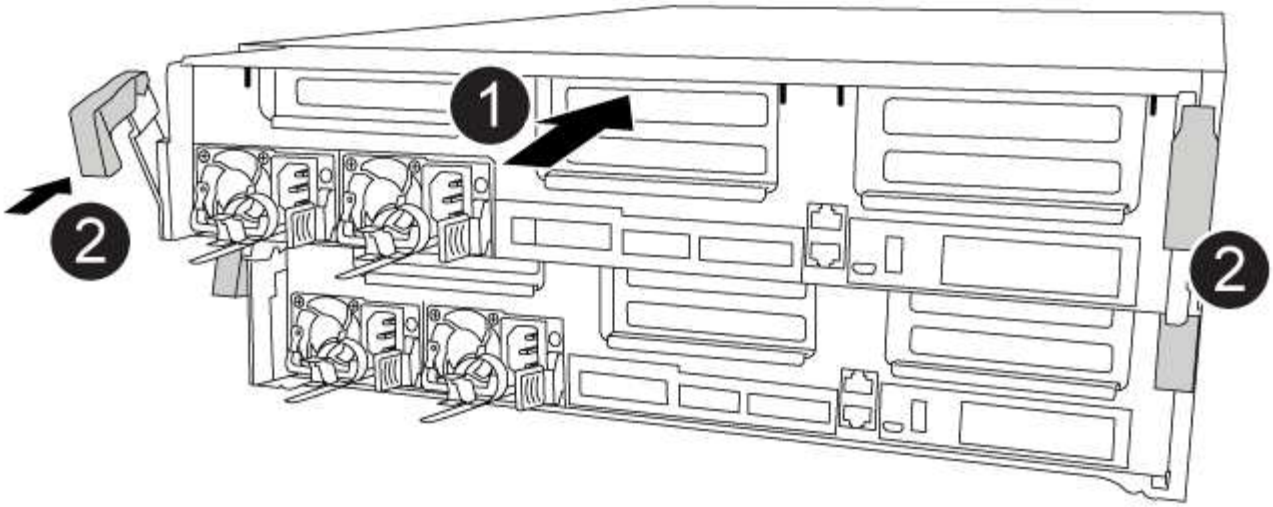
7. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
8. Close the air duct.

#### Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, drawing, or the written steps to install the controller module in the chassis.

Installing the controller module




**Steps**

1. If you have not already done so, close the air duct.
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. 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.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

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

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

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

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

> If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.

g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

   If your system stops at the boot menu, select the option to boot to LOADER.

#### Step 5: Run diagnostics

## After you have replaced a system DIMM in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

**Steps**

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.
5. Select an option from the displayed sub-menu and run the test.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select `Reboot` from the menu to reboot the system.

#### Step 6: Restore the controller module to operation after running diagnostics

## After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

**Steps**

1. 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.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

#### Step 7: Switch back aggregates in a two-node MetroCluster configuration

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

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 8: 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 & Replacements page for further information.

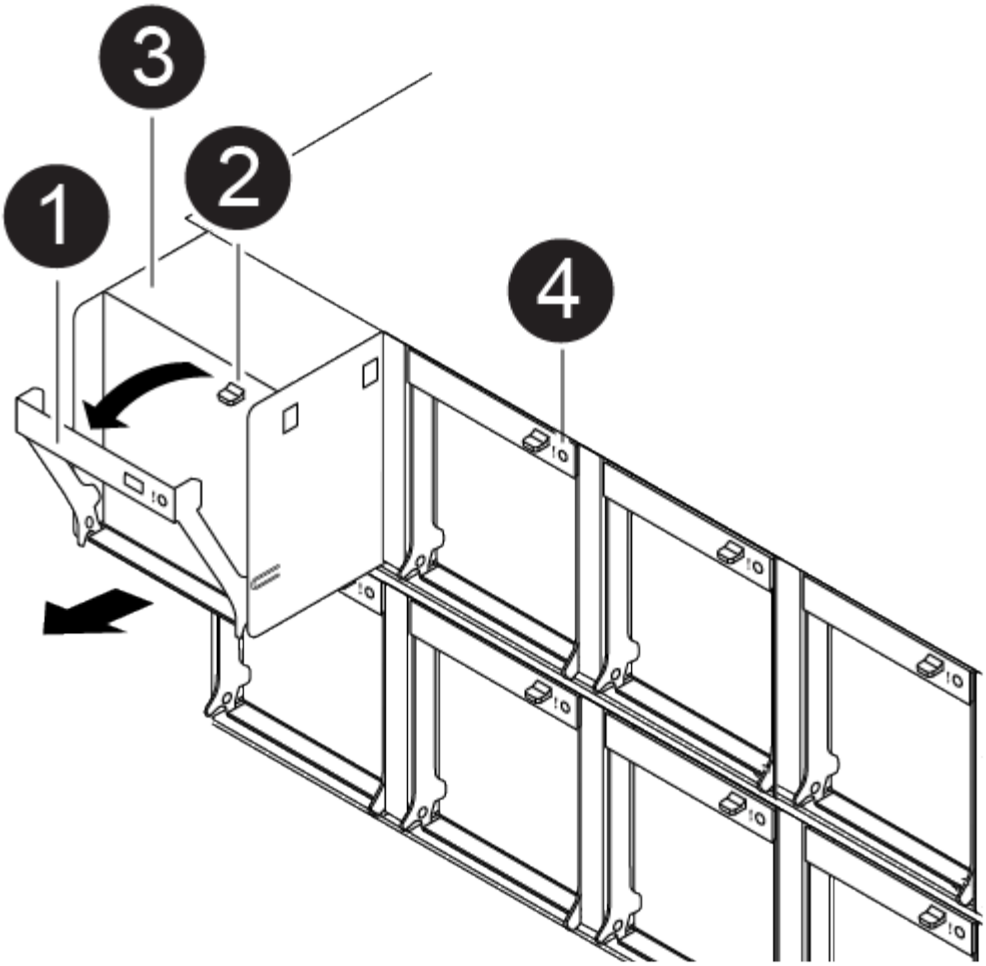
### Hot-swap a fan module - FAS8300 and FAS8700

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.

You can use the following animation, illustration, or the written steps to hot-swap a fan module.

Replacing a fan




**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 down the release latch on the fan module cam handle, and then rotate the cam handle downward.

   The fan module moves a little bit away from the chassis.

5. Pull the fan module straight out from the chassis, making sure that you support it with your free hand so that it does not swing out of the chassis.

   > 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.

6. Set the fan module aside.
7. Insert the replacement fan module into the chassis by aligning it with the opening, and then sliding it into the chassis.
8. Push firmly on the fan module cam handle so that it is seated all the way into the chassis.

The cam handle raises slightly when the fan module is completely seated.

9. Swing the cam handle up to its closed position, making sure that the cam handle release latch clicks into the locked position.

   The Attention LED should not be lit after the fan is seated and has spun up to operational speed.

10. Align the bezel with the ball studs, and then gently push the bezel onto the ball studs.
11. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Replace an NVDIMM - FAS8300 and FAS8700

You must replace the NVDIMM in the controller module when your system registers that the flash lifetime is almost at an end or that the identified NVDIMM is not healthy in general; failure to do so causes a system panic.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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: -
```

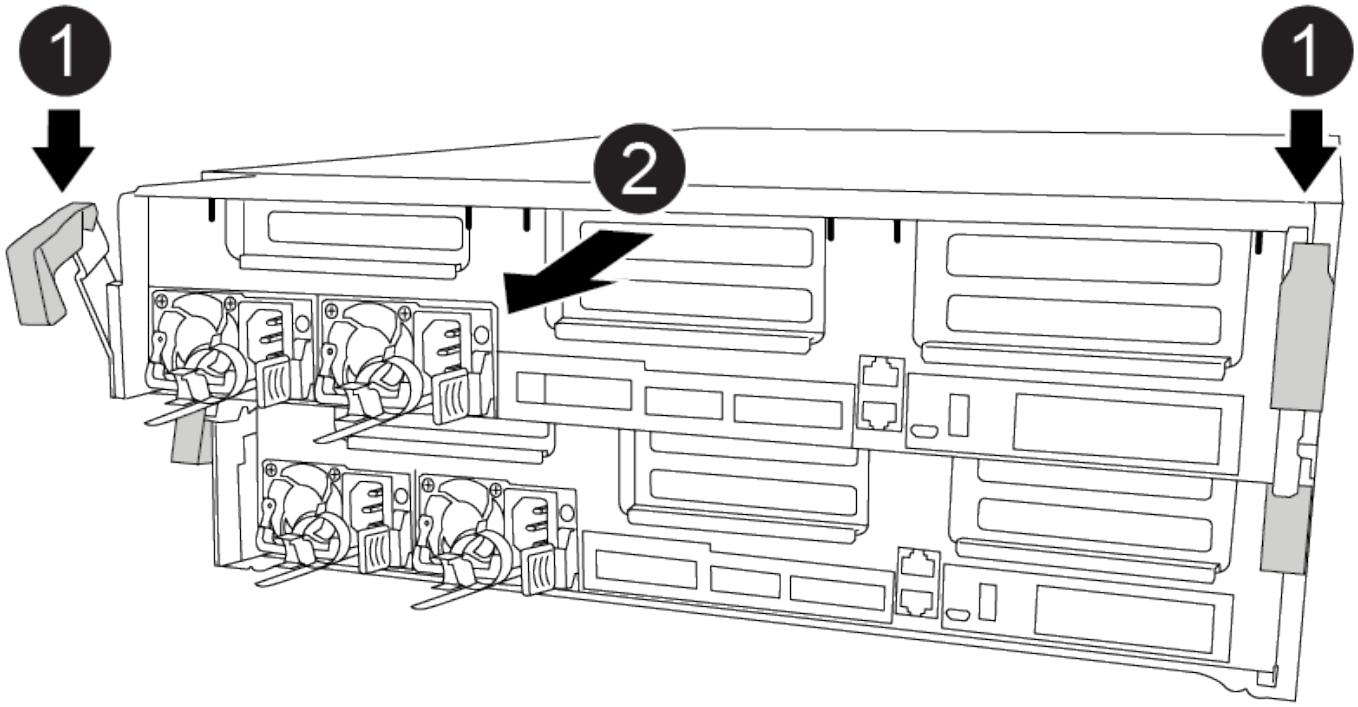
8. On the impaired controller module, disconnect the power supplies.

#### Step 2: Remove the controller module

## To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following , illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module




**Steps**

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. 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.

7. Place the controller module on a stable, flat surface.

#### Step 3: Replace the NVDIMM

To replace the NVDIMM, you must locate it in the controller module using the FRU map on top of the air duct or locate the Attention LED using the FRU Map on the top of the slot 1 riser.

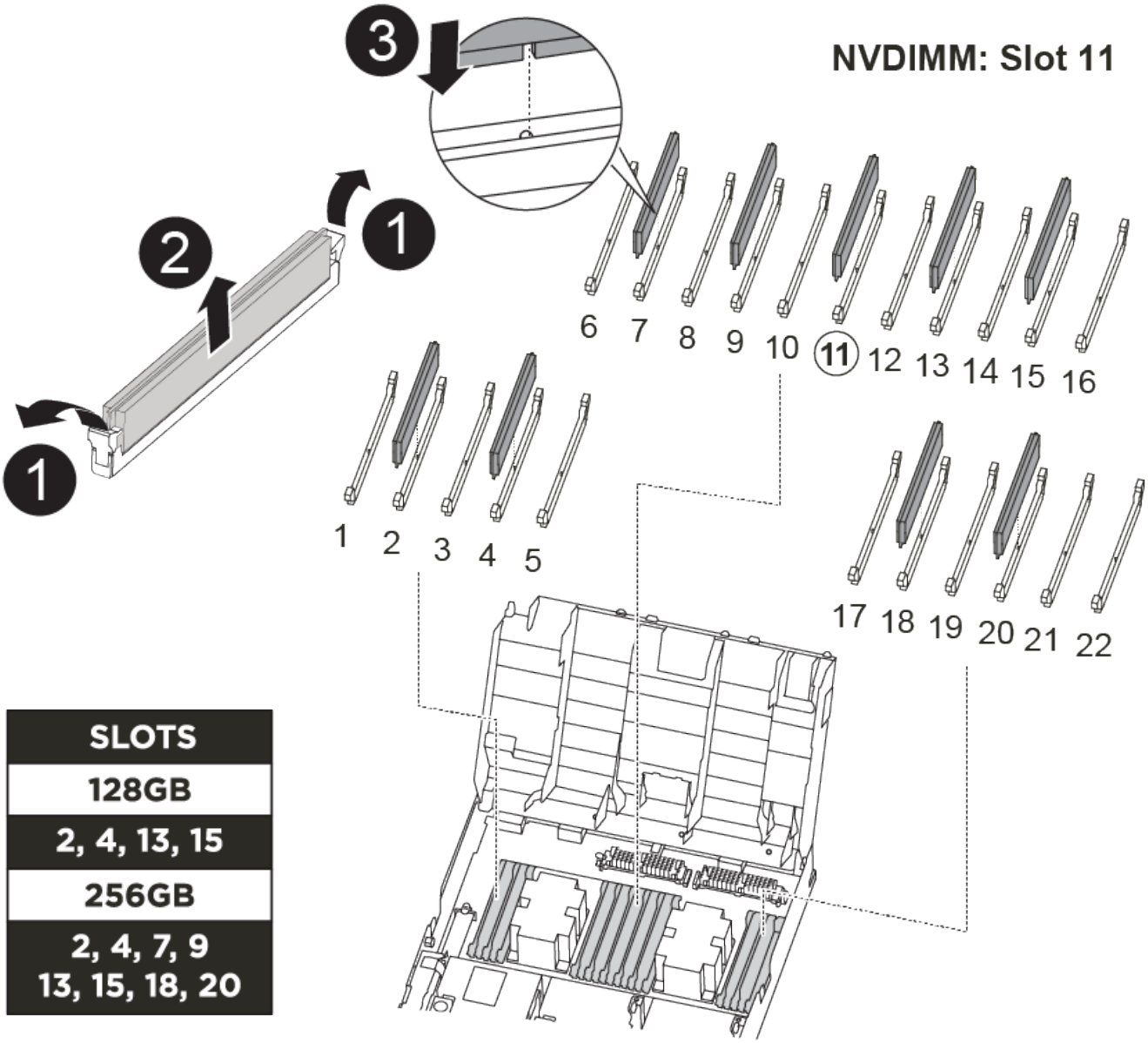
- The NVDIMM LED blinks while destaging contents when you halt the system. After the destage is complete, the LED turns off.
- Although the contents of the NVDIMM is encrypted, it is a best practice to erase the contents of the NVDIMM before replacing it. For more information, see the Statement of Volatility on the NetApp Support Site.

> You must log into the NetApp Support Site to display the *Statement of Volatility* for your system.

You can use the following animation, illustration, or the written steps to replace the NVDIMM.

> The animation and illustration show empty slots for sockets without DIMMs. These empty sockets are populated with blanks.

Replacing the NVDIMM




**Steps**

1. Open the air duct and then locate the NVDIMM in slot 11 on your controller module.

   The NVDIMM looks significantly different than system DIMMs.

2. Eject the NVDIMM from its slot by slowly pushing apart the two NVDIMM ejector tabs on either side of the NVDIMM, and then slide the NVDIMM out of the socket and set it aside.

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

3. Remove the replacement NVDIMM from the antistatic shipping bag, hold the NVDIMM by the corners, and then align it to the slot.

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

4. Locate the slot where you are installing the NVDIMM.
5. Insert the NVDIMM squarely into the slot.

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

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

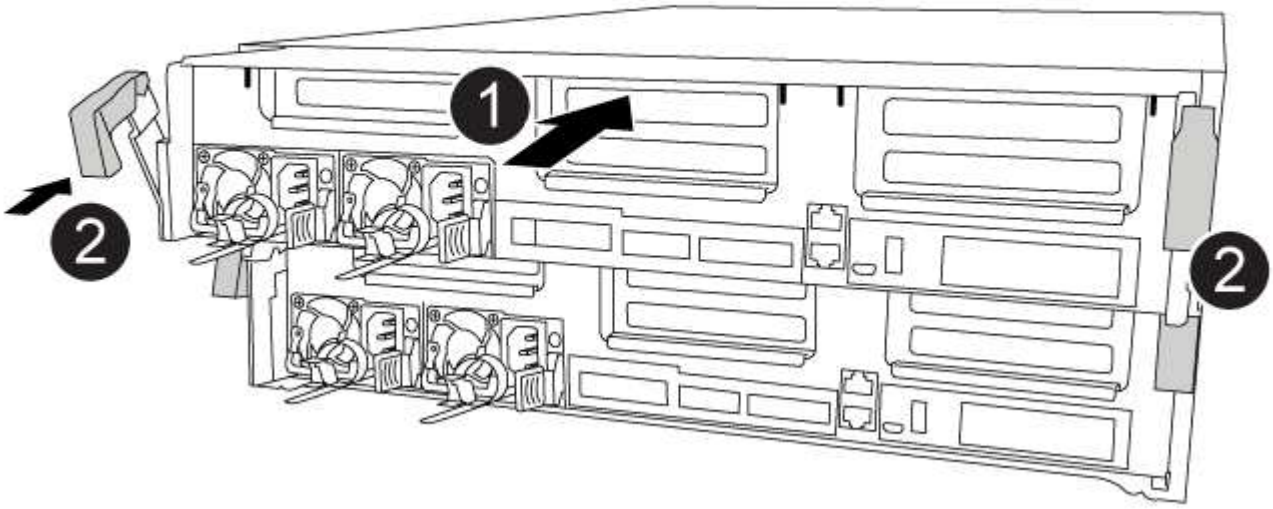
6. Push carefully, but firmly, on the top edge of the NVDIMM until the ejector tabs snap into place over the notches at the ends of the NVDIMM.
7. Close the air duct.

#### Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module




**Steps**

1. If you have not already done so, close the air duct.
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. 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.

4. Complete the installation of the controller module:
   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
   b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

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

   c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

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

   d. If you have not already done so, reinstall the cable management device.
   e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      > If your system stops at the boot menu, select the option to boot to LOADER.

   f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.
   g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

      If your system stops at the boot menu, select the option to boot to LOADER.

#### Step 5: Run diagnostics

After you have replaced the NVDIMM in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

**Steps**

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node` *`node_name`*

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu.

5. Select **NVDIMM Test** from the displayed menu.
6. Proceed based on the result of the preceding step:
   - If the test failed, correct the failure, and then rerun the test.
   - If the test reported no failures, select `Reboot` from the menu to reboot the system.

#### Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

**Steps**

1. 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.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` `impaired_node_name`
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

#### Step 7: Switch back aggregates in a two-node MetroCluster configuration

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

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 8: 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 & Replacements page for further information.

### Replace the NVDIMM battery - FAS8300 and FAS8700

To replace the NVDIMM battery, you must remove the controller module, remove the battery, replace the battery, and then reinstall the controller module.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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: -
```

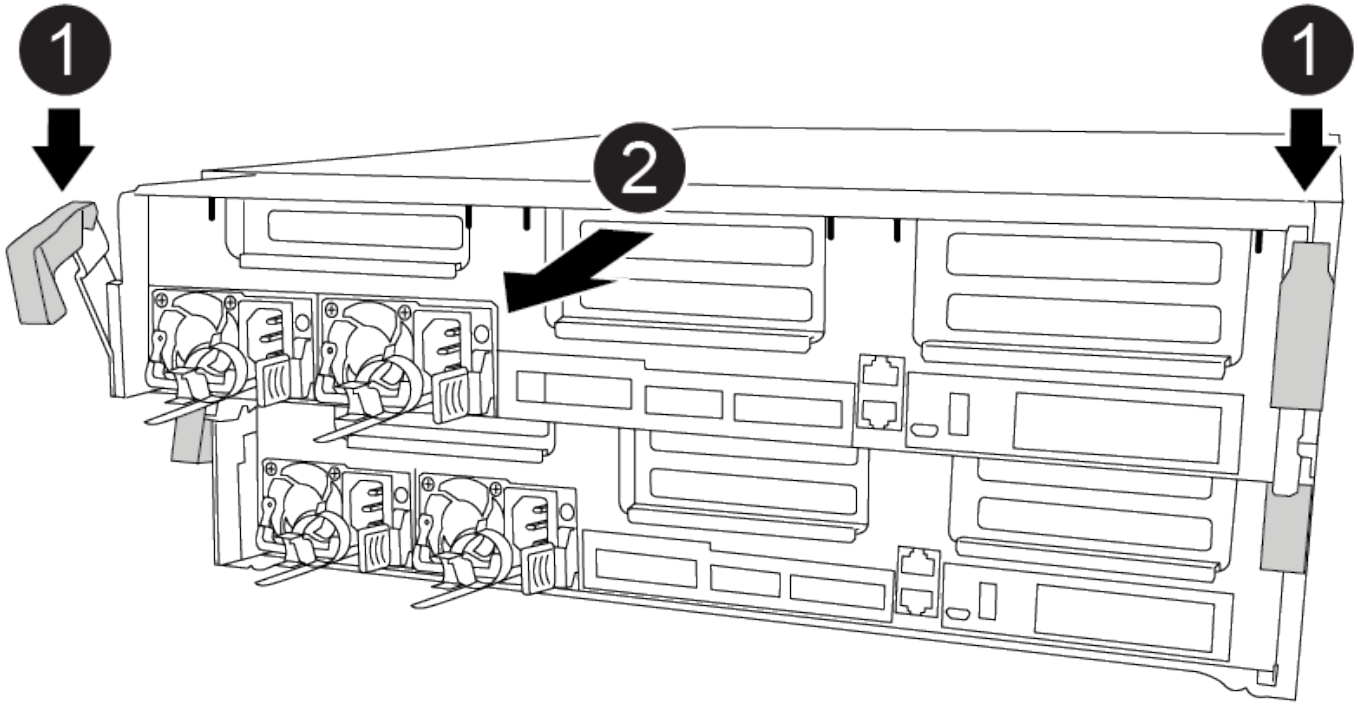
8. On the impaired controller module, disconnect the power supplies.

#### Step 2: Remove the controller module

## To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module




**Steps**

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. 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.

7. Place the controller module on a stable, flat surface.

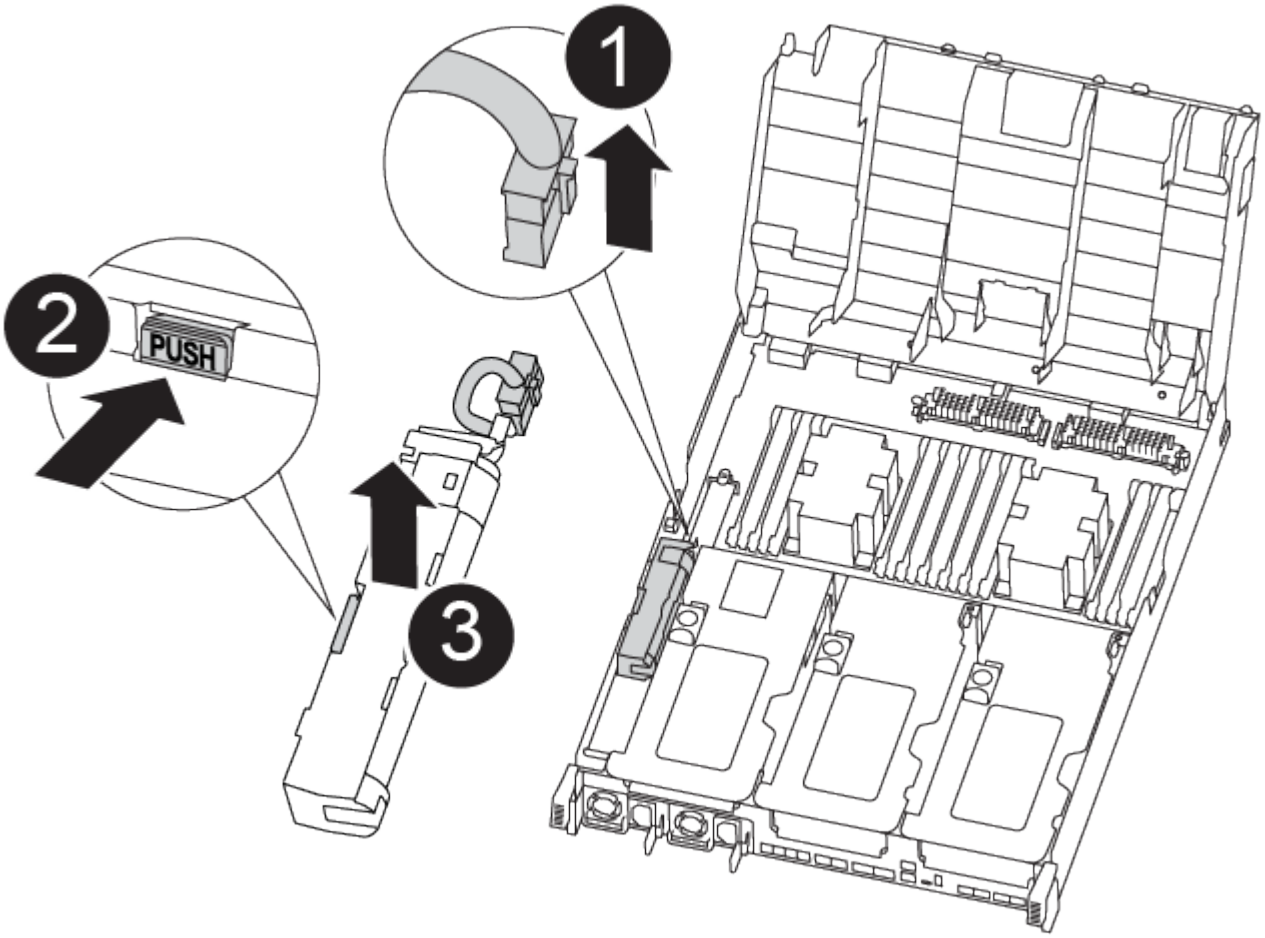
#### Step 3: Replace the NVDIMM battery

To replace the NVDIMM battery, you must remove the failed battery from the controller module and install the replacement battery into the controller module. See the FRU map inside the controller module to locate the NVDIMM battery.

The NVDIMM LED blinks while destaging contents when you halt the system. After the destage is complete, the LED turns off.

You can use the following animation, illustration, or the written steps to replace the NVDIMM battery.

Replacing the NVDIMM battery




**Steps**

1. Open the air duct:
   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
   b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
2. Locate the NVDIMM battery in the controller module.
3. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the

socket, and then unplug the battery cable from the socket.

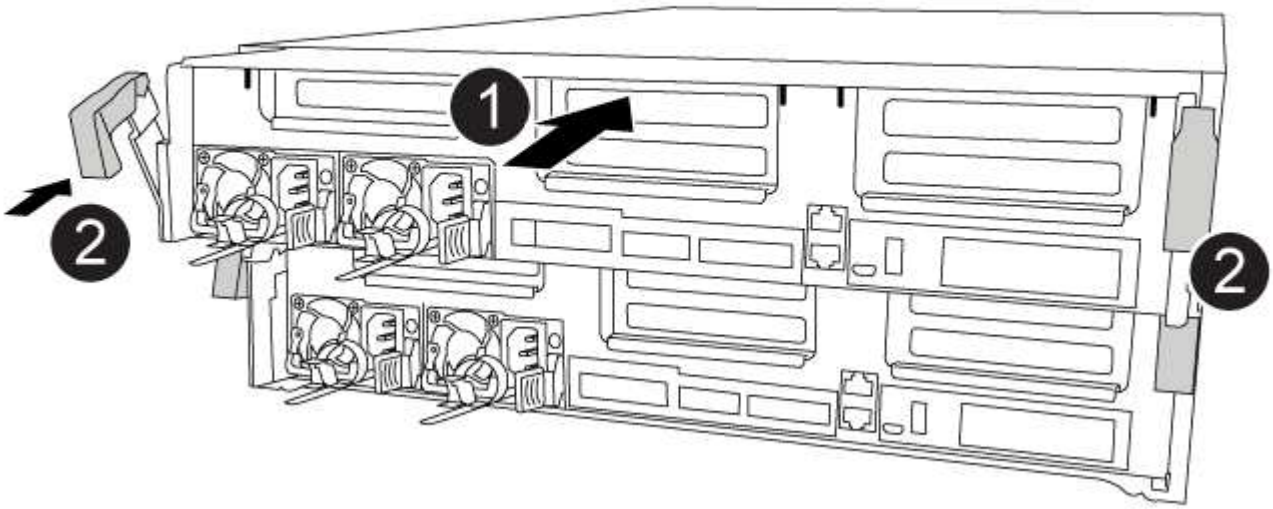
4. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module.
5. Remove the replacement battery from its package.
6. Align the battery module with the opening for the battery, and then gently push the battery into slot until it locks into place.
7. Plug the battery plug back into the controller module, and then close the air duct.

#### Step 4: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module




**Steps**

1. If you have not already done so, close the air duct.
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. 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.

4. Complete the installation of the controller module:

a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.

b. Using the locking latches, firmly push the controller module into the chassis until the locking latches begin to rise.

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

c. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

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

d. If you have not already done so, reinstall the cable management device.

e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

> If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components.

g. Interrupt the boot process and boot to the LOADER prompt by pressing `Ctrl-C`.

   If your system stops at the boot menu, select the option to boot to LOADER.

#### Step 5: Run diagnostics

After you have replaced a component in your system, you should run diagnostic tests on that component.

Your system must be at the LOADER prompt to start diagnostics.

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

**Steps**

1. If the controller to be serviced is not at the LOADER prompt, reboot the controller: `system node halt -node node_name`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`
3. Select **Scan System** from the displayed menu to enable running the diagnostics tests.
4. Select **Test Memory** from the displayed menu to run diagnostics tests.
5. Proceed based on the result of the preceding step:
   - If the scan show problems, correct the issue, and then rerun the scan.
   - If the scan reported no failures, select `Reboot` from the menu to reboot the system.

#### Step 6: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

**Steps**

1. 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.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

#### Step 7: Switch back aggregates in a two-node MetroCluster configuration

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

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 8: 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 & Replacements page for further information.

### Replace a PCIe or mezzanine card - FAS8300 and FAS8700

To replace a PCIe or mezzanine card, you must disconnect the cables and any SFP and QSFP modules from the cards, replace the failed PCIe or mezzanine card, and then recable the cards.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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: -
```

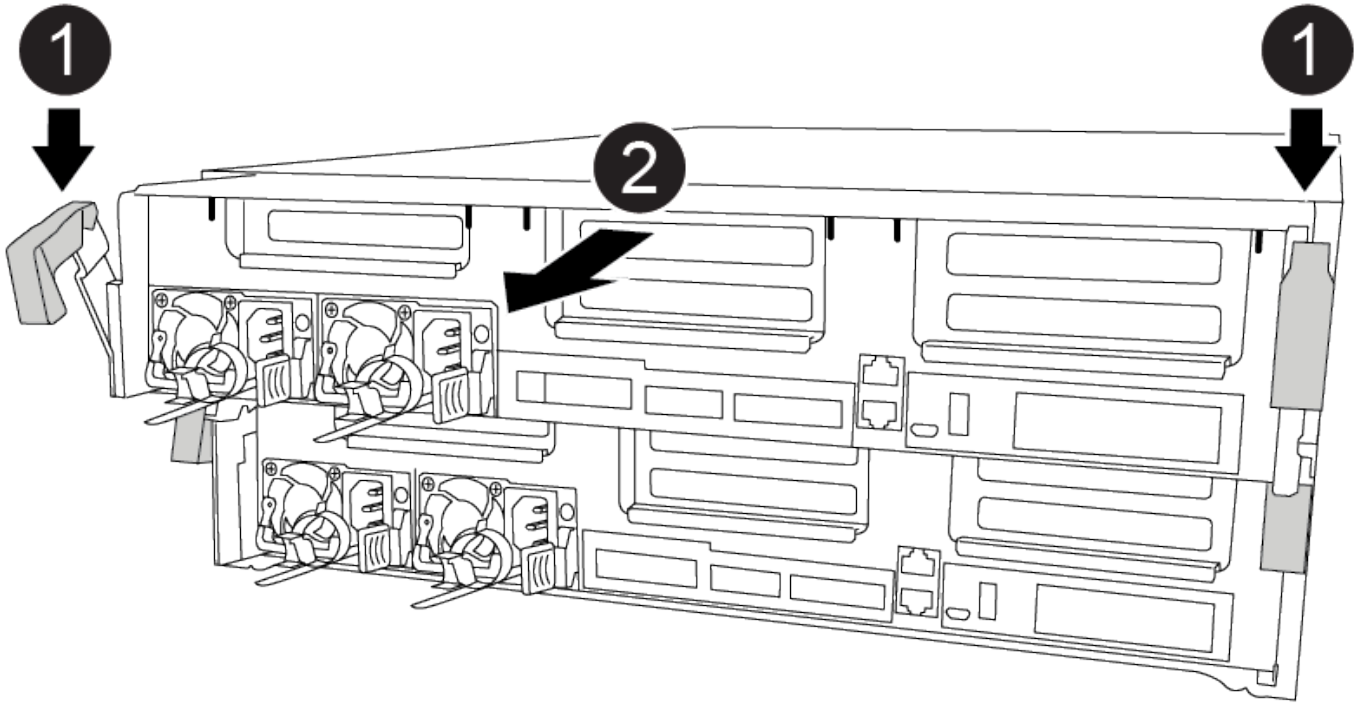
8. On the impaired controller module, disconnect the power supplies.

#### Step 2: Remove the controller module

## To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module




**Steps**

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. 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.

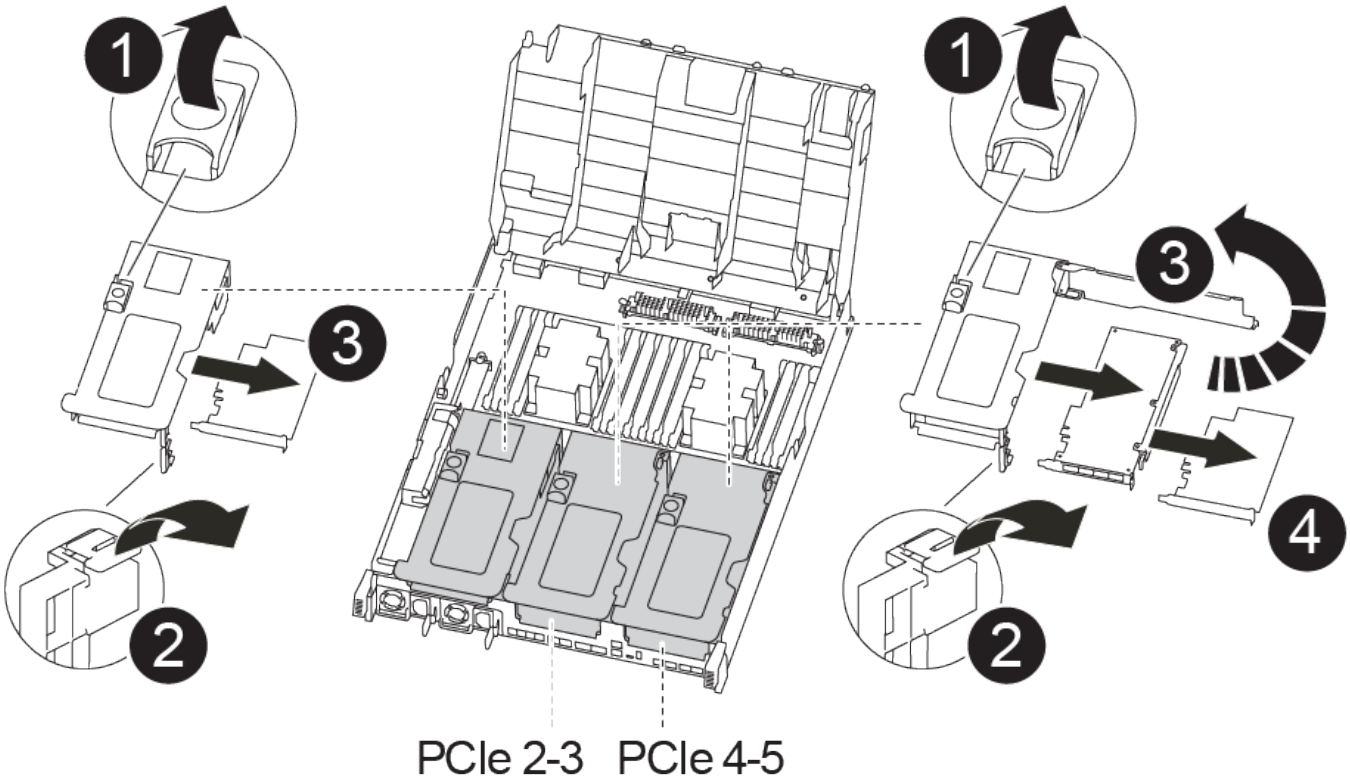
7. Place the controller module on a stable, flat surface.

#### Step 3: Replace a PCIe card

To replace a PCIe card, you must locate the failed PCIe card, remove the riser that contains the card from the controller module, replace the card, and then reinstall the PCIe riser in the controller module.

You can use the following animation, illustration, or the written steps to replace a PCIe card.

Replacing a PCIe card




**Steps**

1. Remove the riser containing the card to be replaced:
   a. Open the air duct by pressing the locking tabs on the sides of the air duct, slide it toward the back of the controller module, and then rotate it to its completely open position.
   b. Remove any SFP or QSFP modules that might be in the PCIe cards.
   c. Rotate the riser locking latch on the left side of the riser up and toward air duct.

      The riser raises up slightly from the controller module.

   d. Lift the riser up straight up and set it aside on a stable flat surface,
2. Remove the PCIe card from the riser:
   a. Turn the riser so that you can access the PCIe card.
   b. Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.

c. For risers 2 and 3 only, swing the side panel up.

d. Remove the PCIe card from the riser by gently pushing up on the bracket and lift the card straight out of the socket.

3. Install the replacement PCIe card in the riser by aligning the card with the socket, press the card into the socket and then close the side panel on the riser, if present.

   Be sure that you properly align the card in the slot and exert even pressure on the card when seating it in the socket. The PCIe card must be fully and evenly seated in the slot.

   > If you are installing a card in the bottom slot and cannot see the card socket well, remove the top card so that you can see the card socket, install the card, and then reinstall the card you removed from the top slot.

4. Reinstall the riser:

   a. Align the riser with the pins to the side of the riser socket, lower the riser down on the pins.

   b. Push the riser squarely into the socket on the motherboard.

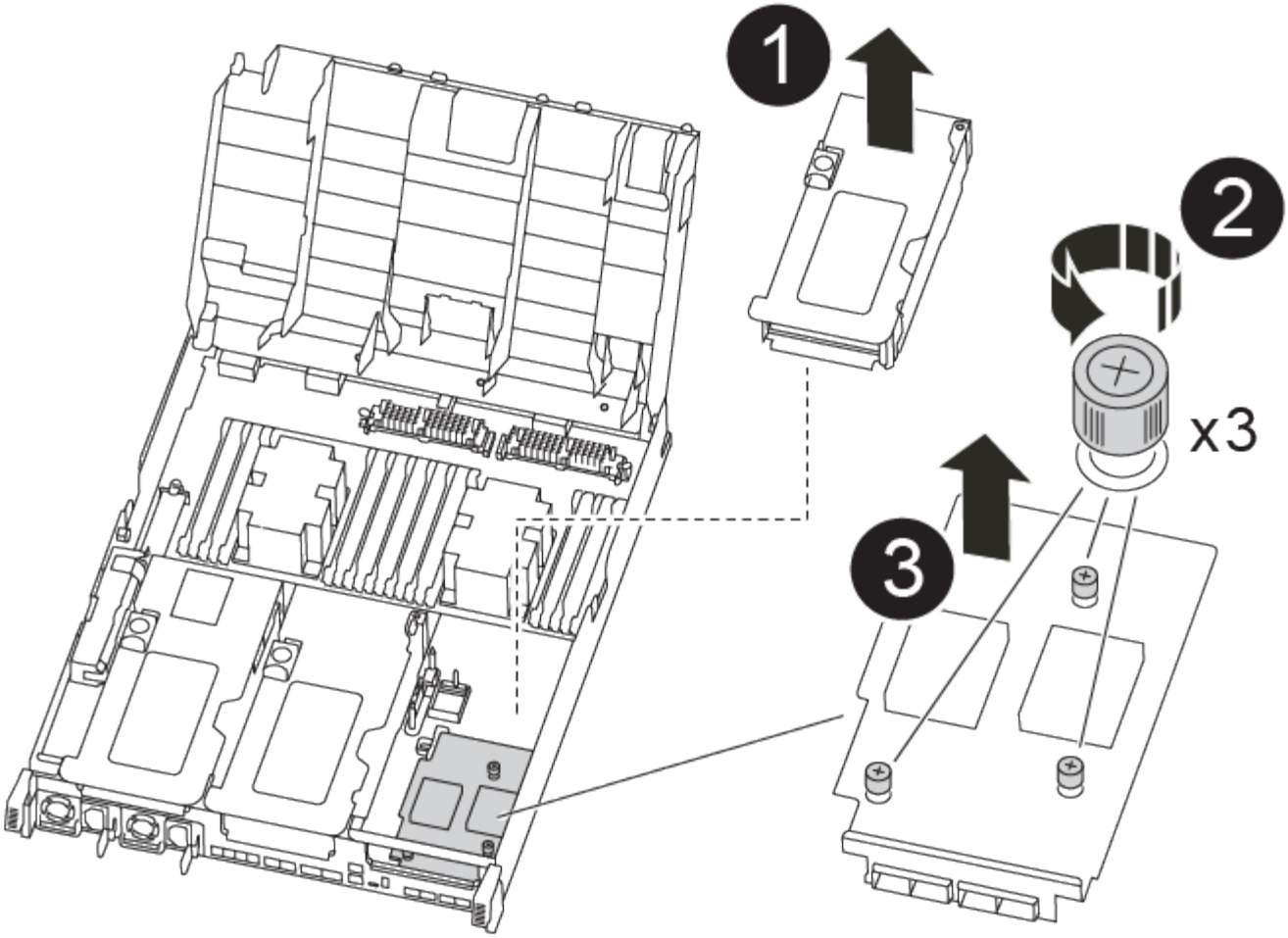
   c. Rotate the latch down flush with the sheet metal on the riser.

#### Step 4: Replace the mezzanine card

The mezzanine card is located under riser number 3 (slots 4 and 5). You must remove that riser to access the mezzanine card, replace the mezzanine card, and then reinstall riser number 3. See the FRU map on the controller module for more information.

You can use the following animation, illustration, or the written steps to replace the mezzanine card.

Replacing the mezzanine card




**Steps**

1. Remove riser number 3 (slots 4 and 5):
   a. Open the air duct by pressing the locking tabs on the sides of the air duct, slide it toward the back of the controller module, and then rotate it to its completely open position.
   b. Remove any SFP or QSFP modules that might be in the PCIe cards.
   c. Rotate the riser locking latch on the left side of the riser up and toward air duct.

      The riser raises up slightly from the controller module.

   d. Lift the riser up, and then set it aside on a stable, flat surface.
2. Replace the mezzanine card:
   a. Remove any QSFP or SFP modules from the card.
   b. Loosen the thumbscrews on the mezzanine card, and gently lift the card directly out of the socket and set it aside.
   c. Align the replacement mezzanine card over the socket and the guide pins and gently push the card into the socket.
   d. Tighten the thumbscrews on the mezzanine card.
3. Reinstall the riser:
   a. Align the riser with the pins to the side of the riser socket, lower the riser down on the pins.

b. Push the riser squarely into the socket on the motherboard.

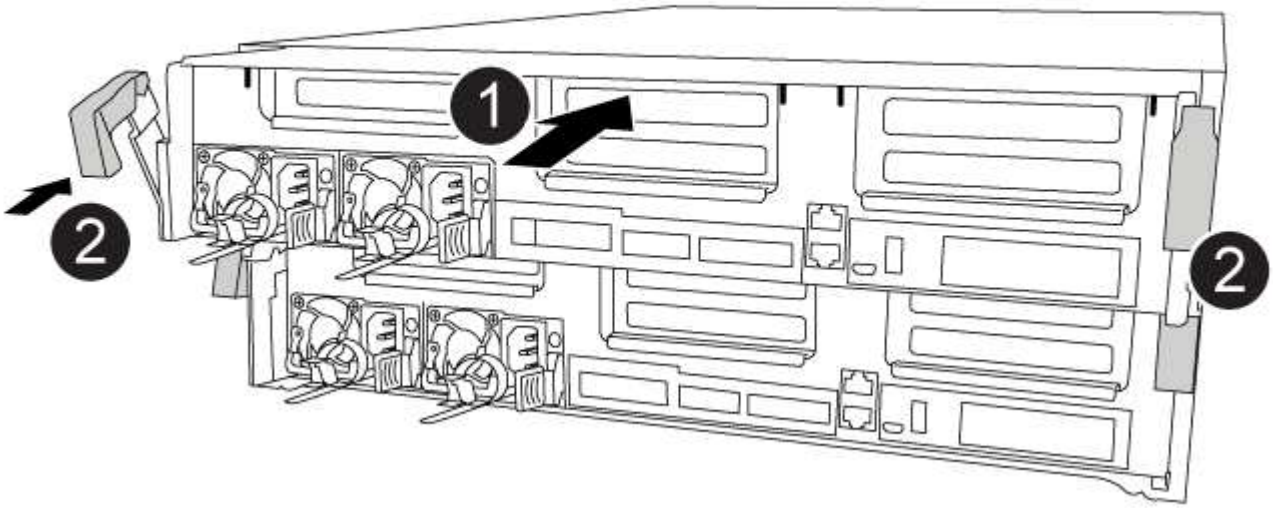
c. Rotate the latch down flush with the sheet metal on the riser.

#### Step 5: Install the controller module

After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it to Maintenance mode.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module




**Steps**

1. If you have not already done so, close the air duct.
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. Complete the installation of the controller module:

   a. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.

   b. Using the locking latches, 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. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.

d. If you have not already done so, reinstall the cable management device.

e. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

> If your system stops at the boot menu, select the option to boot to LOADER.

f. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.

5. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode` *`impaired_node_name`*

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

#### Step 6: Switch back aggregates in a two-node MetroCluster configuration

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

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 7: Restore the controller module to operation after running diagnostics

After completing diagnostics, you must recable the system, give back the controller module, and then reenable automatic giveback.

**Steps**

1. 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.

2. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

#### Step 8: 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 & Replacements page for further information.

### Replace a power supply - FAS8300 and FAS8700

Replacing a power supply (PSU) involves disconnecting the target PSU from the power source, unplugging the power cable, removing the old PSU and installing the replacement PSU, and then reconnecting the replacement PSU to the power source.

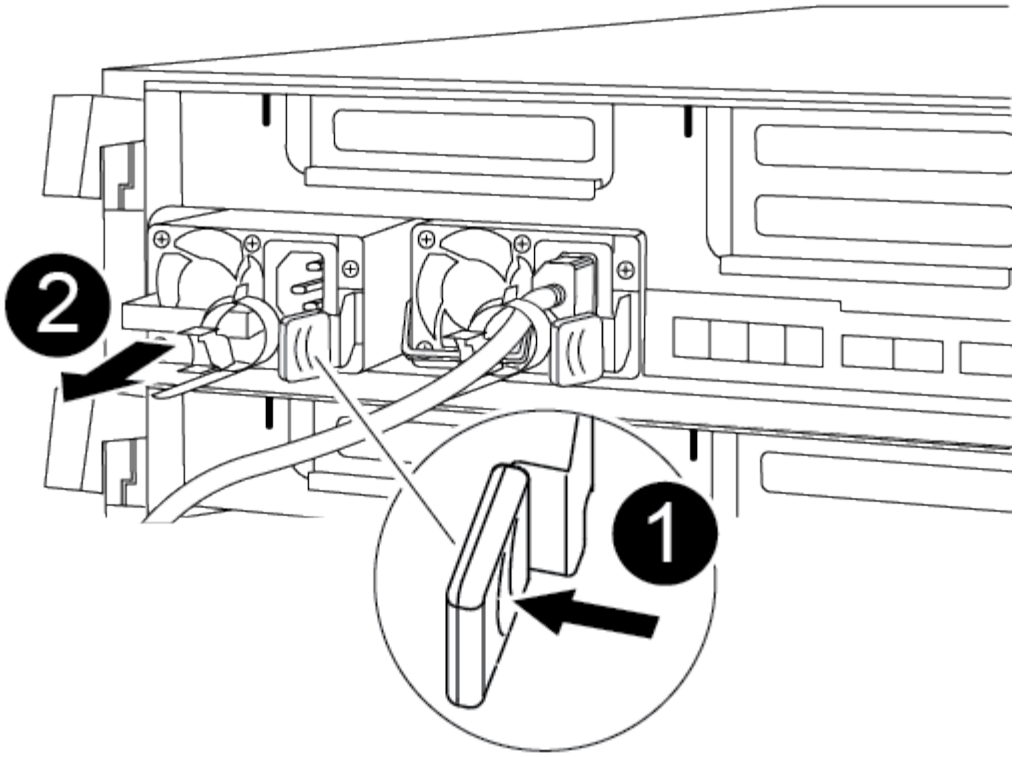
- The power supplies are redundant and hot-swappable.
- This procedure is written for replacing one power supply at a time.

> 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.

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

You can use the following animation, illustration, or the written steps to replace the power supply.

Replacing a power supply




**Steps**

1. If you are not already grounded, properly ground yourself.
2. Identify the power supply you want to replace, based on console error messages or through the LEDs on the power supplies.
3. Disconnect the power supply:
   a. Open the power cable retainer, and then unplug the power cable from the power supply.
   b. Unplug the power cable from the power source.
4. Remove the power supply:
   a. Rotate the cam handle so that it can be used to pull the power supply out of the chassis.
   b. Press the blue locking tab to release the power supply from the chassis.
   c. Using both hands, pull the power supply out of the chassis, and then set it aside.
5. Using both hands, support and align the edges of the power supply with the opening in the controller module, and then gently push the power supply into the controller module until the locking tab clicks into place.

   The power supplies will only properly engage with the internal connector and lock in place one way.

   > To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

6. Rotate the cam handle so that it is flush against the power supply.
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. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Replace the real-time clock battery - FAS8300 and FAS8700

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.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

**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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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: -
```

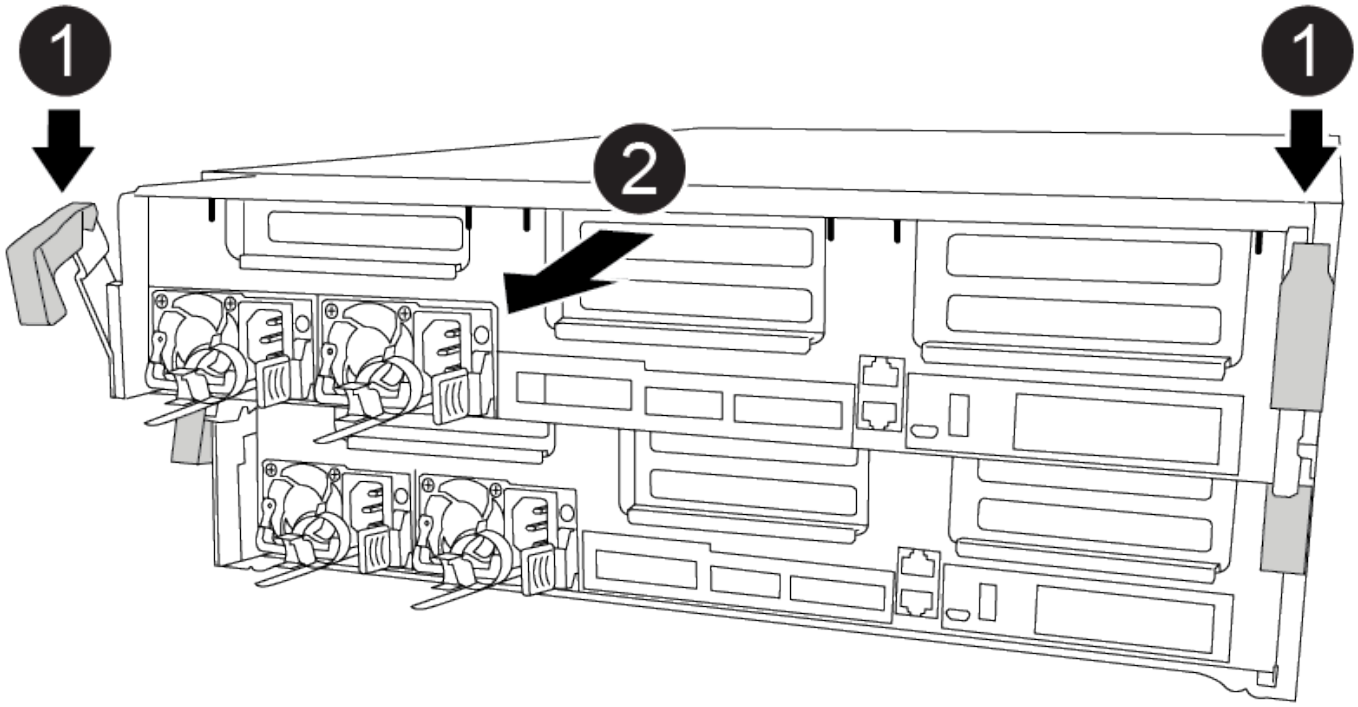
8. On the impaired controller module, disconnect the power supplies.

**Step 2: Remove the controller module**

## To access components inside the controller module, you must remove the controller module from the chassis.

You can use the following animation, illustration, or the written steps to remove the controller module from the chassis.

Removing the controller module




**Steps**

1. If you are not already grounded, properly ground yourself.
2. Release the power cable retainers, and then unplug the cables from the power supplies.
3. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFPs (if needed) from the controller module, keeping track of where the cables were connected.

   Leave the cables in the cable management device so that when you reinstall the cable management device, the cables are organized.

4. Remove the cable management device from the controller module and set it aside.
5. Press down on both of the locking latches, and then rotate both latches downward at the same time.

   The controller module moves slightly out of the chassis.

6. 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.

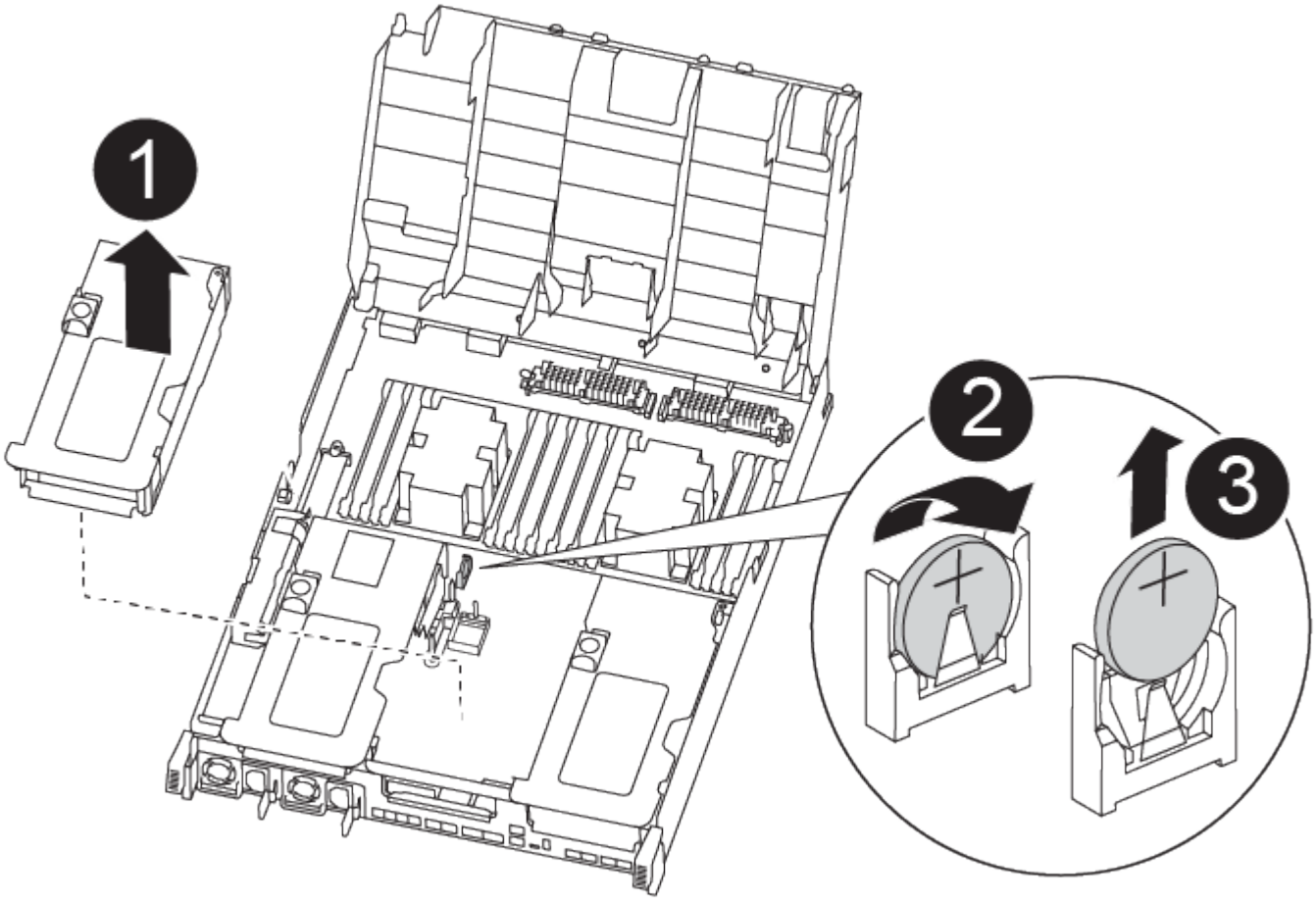
7. Place the controller module on a stable, flat surface.

#### Step 3: Replace the RTC battery

You need to locate the RTC battery inside the controller module, and then follow the specific sequence of steps. See the FRU map inside the controller module for the location of the RTC battery.

You can use the following animation, illustration, or the written steps to replace the RTC battery.

Replacing the RTC battery




**Steps**

1. If you are not already grounded, properly ground yourself.
2. Open the air duct:
   a. Press the locking tabs on the sides of the air duct in toward the middle of the controller module.
   b. Slide the air duct toward the back of the controller module, and then rotate it upward to its completely open position.
3. Locate, remove, and then replace the RTC battery:
   a. Using the FRU map, locate the RTC battery on the controller module.
   b. 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.

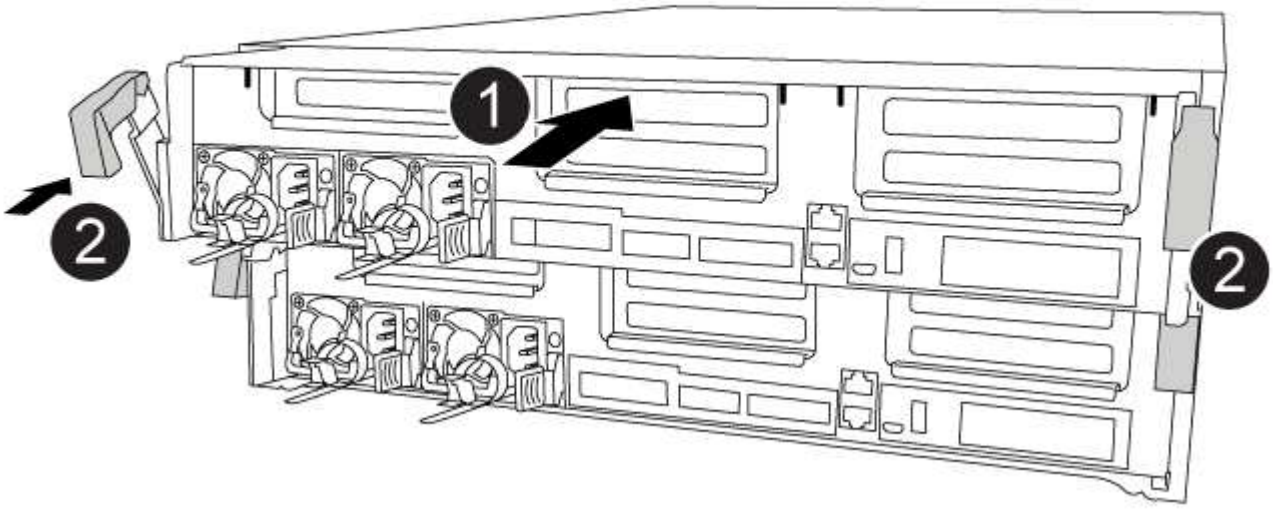
   c. Remove the replacement battery from the antistatic shipping bag.
   d. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
4. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.
5. Close the air duct.

#### Step 4: Reinstall the controller module and sett time/date after RTC battery replacement

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.

You can use the following animation, illustration, or the written steps to install the controller module in the chassis.

Installing the controller module




**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 installation of the controller module:
   a. Using the locking latches, 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.

   b. Fully seat the controller module in the chassis by rotating the locking latches upward, tilting them so that they clear the locking pins, gently push the controller all the way in, and then lower the locking latches into the locked position.
   c. If you have not already done so, reinstall the cable management device.
   d. Interrupt the normal boot process and boot to LOADER by pressing `Ctrl-C`.

      > If your system stops at the boot menu, select the option to boot to LOADER.

6. Reset the time and date on the controller:
   a. Check the date and time on the healthy controller with the `show date` command.
   b. At the LOADER prompt on the target controller, 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 controller.
7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
8. Return the controller 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

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

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 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 & Replacements page for further information.

# FAS9000 System Documentation

## Install and setup

#### Start here: Choose your installation and setup experience

For most configurations, you can choose from different content formats.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

For MetroCluster configurations, see either:

- Install MetroCluster IP configuration
- Install MetroCluster Fabric-Attached configuration

#### Quick steps - AFF A700 and FAS9000

This guide gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this guide if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

AFF A700 Installation and Setup Instructions

FAS9000 Installation and Setup Instructions

#### Video steps - AFF A700 and FAS9000

There are two videos; one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

#### Video one of two: Hardware installation and cabling

The following video shows how to install and cable your new system.

Installation and setup of an AFF A700 or FAS9000

#### Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.2 and later.

NetApp video: Software configuration for vSphere NAS datastores for FAS/AFF systems running ONTAP 9.2

### Detailed guide - AFF A700 and FAS9000

This guide gives detailed step-by-step instructions for installing a typical NetApp system. Use this guide if you want more detailed installation instructions.

#### Step 1: Prepare for installation

To install your system, you need to create an account on the NetApp Support Site, register your system, and get license keys. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

**Before you begin**

You need to have access to the Hardware Universe for information about site requirements as well as additional information on your configured system. You might also want to have access to the Release Notes for your version of ONTAP for more information about this system.

NetApp Hardware Universe

Find the Release Notes for your version of ONTAP 9

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser

**Steps**

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the Hardware Universe to locate the cable and identify its use.

   NetApp Hardware Universe

| Type of cable… | Part number and length | Connector type | For… |
|---|---|---|---|
| 10 GbE network cable | X6566B-2-R6, (112-00299), 2m<br><br>X6566B-3-R6, 112-00300, 3m<br><br>X6566B-5-R6 , 112-00301, 5m | | Network cable |
| 40 GbE network cable<br><br>40 GbE cluster interconnect | X66100-1,112-00542, 1m<br><br>X66100-3,112-00543, 3m | | 40 GbE network<br><br>Cluster interconnect |
| 100 GbE network cable<br><br>100 GbE storage cable | X66211A-05 (112-00595), 0.5m<br><br>X66211A-1 (112-00573), 1m<br><br>X66211A-2 (112-00574), 2m<br><br>X66211A-5 (112-00574), 5m | | Network cable<br><br>Storage cable<br><br>This cable applies to AFF A700 only. |
| Optical network cables (order dependent) | X6553-R6 (112-00188), 2m<br><br>X6536-R6 (112-00090), 5m | | FC host network |
| Cat 6, RJ-45 (order dependent) | Part numbers X6585-R6 (112-00291), 3m<br><br>X6562-R6 (112-00196), 5m | | Management network and Ethernet data |
| Storage | X66031A (112-00436), 1m<br><br>X66032A (112-00437), 2m<br><br>X66033A (112-00438), 3m | | Storage |
| Micro-USB console cable | Not applicable | | Console connection during software setup on non-Windows or Mac laptop/console |
| Power cables | Not applicable | | Powering up the system |

4. Review the *NetApp ONTAP Confiuration Guide* and collect the required information listed in that guide.

   ONTAP Configuration Guide

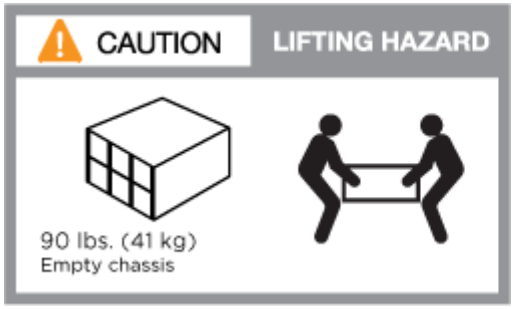
#### Step 2: Install the hardware

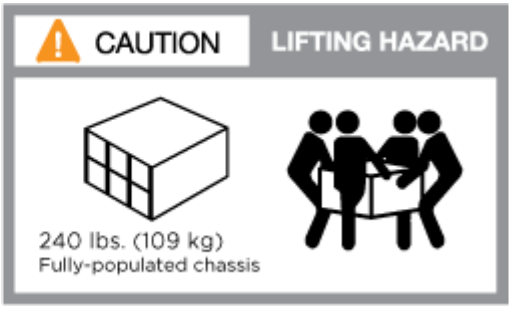
You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

**Steps**

1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

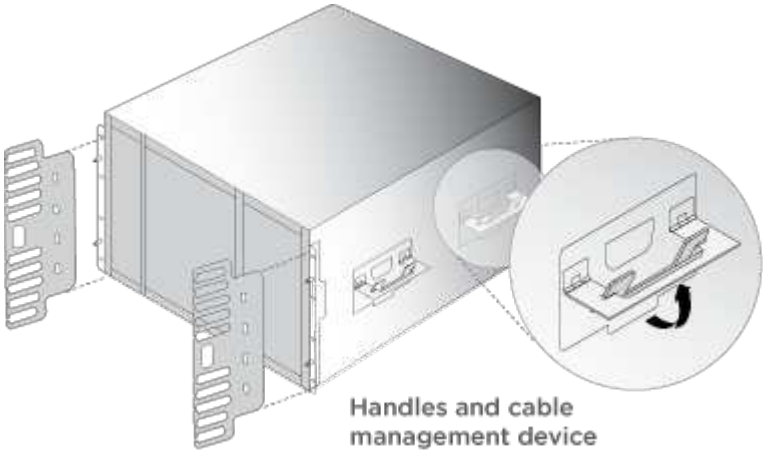
> You need to be aware of the safety concerns associated with the weight of the system.




> The label on the left indicates an empty chassis, while the label on the right indicates a fully-populated system.

1. Attach cable management devices (as shown).




2. Place the bezel on the front of the system.

#### Step 3: Cable controllers to your network

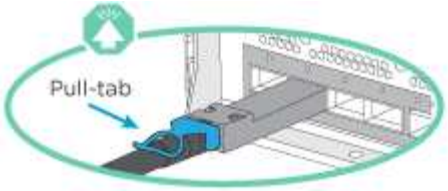
You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

#### Option 1: Two-node switchless cluster

Management network, data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled on both controllers.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all networking module ports.

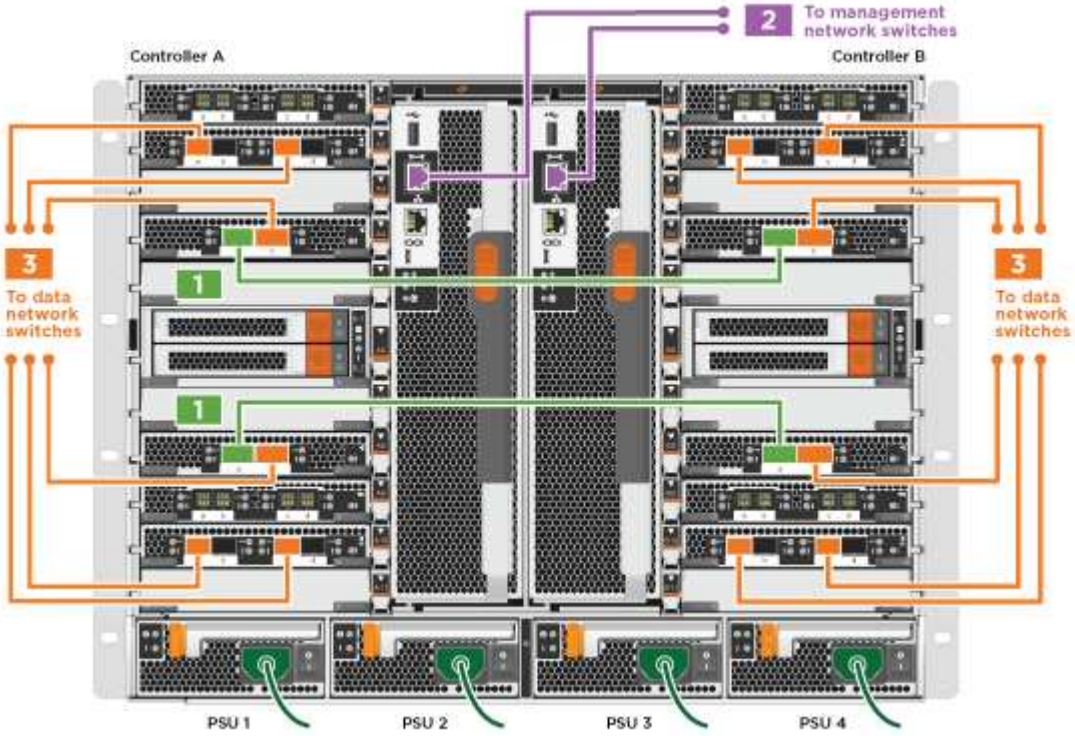



As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Cabling a two-node switchless cluster



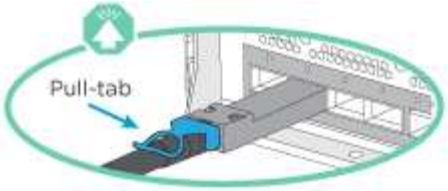

1. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

**Option 2: Switched cluster**

## Management network, data network, and management ports on the controllers are connected to switches. The cluster interconnect and HA ports are cabled on to the cluster/HA switch.

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all networking module ports.

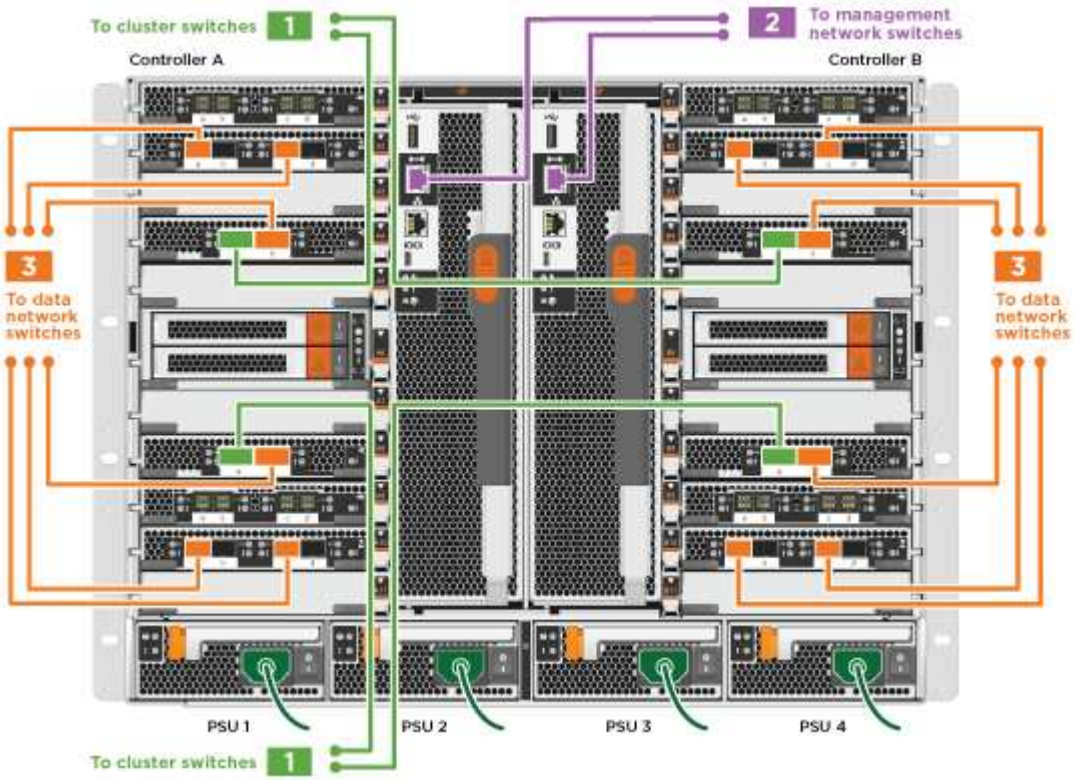



As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

   Switched cluster cabling




1. Go to Step 4: Cable controllers to drive shelves for drive shelf cabling instructions.

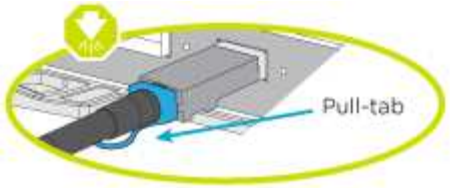
#### Step 4: Cable controllers to drive shelves

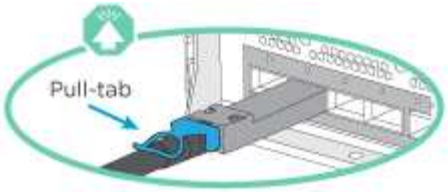
## You can cable your new system to DS212C, DS224C, or NS224 shelves, depending on if it is an AFF or FAS system.

### Option 1: Cable the controllers to DS212C or DS224C drive shelves

## You must cable the shelf-to-shelf connections, and then cable both controllers to the DS212C or DS224C drive shelves.

The cables are inserted into the drive shelf with the pull-tabs facing down, while the other end of the cable is inserted into the controller storage modules with the pull-tabs up.



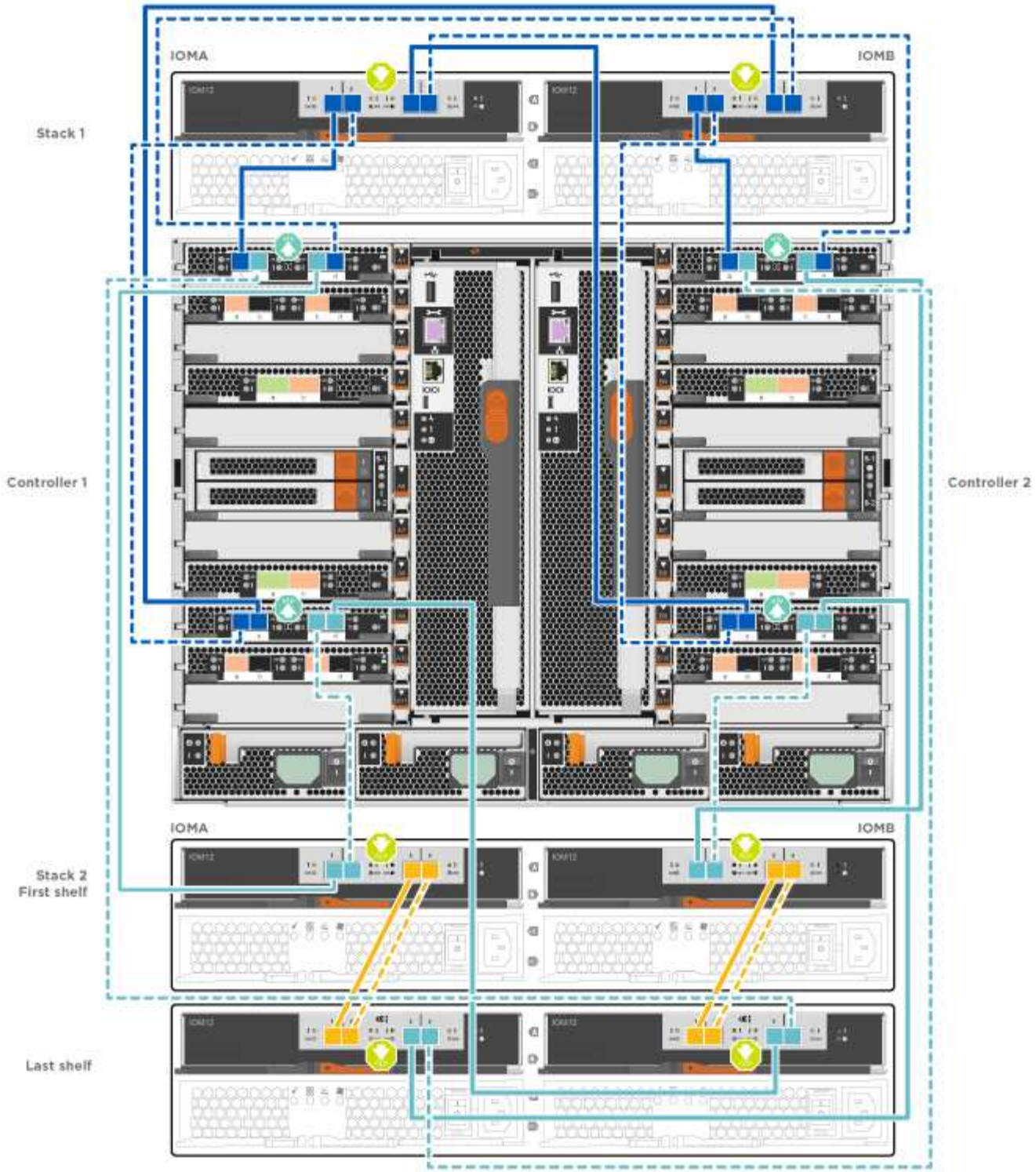

**Steps**

1. Use the following animations or illustrations to cable your drive shelves to your controllers.

> The examples use DS224C shelves. Cabling is similar with other supported SAS drive shelves.

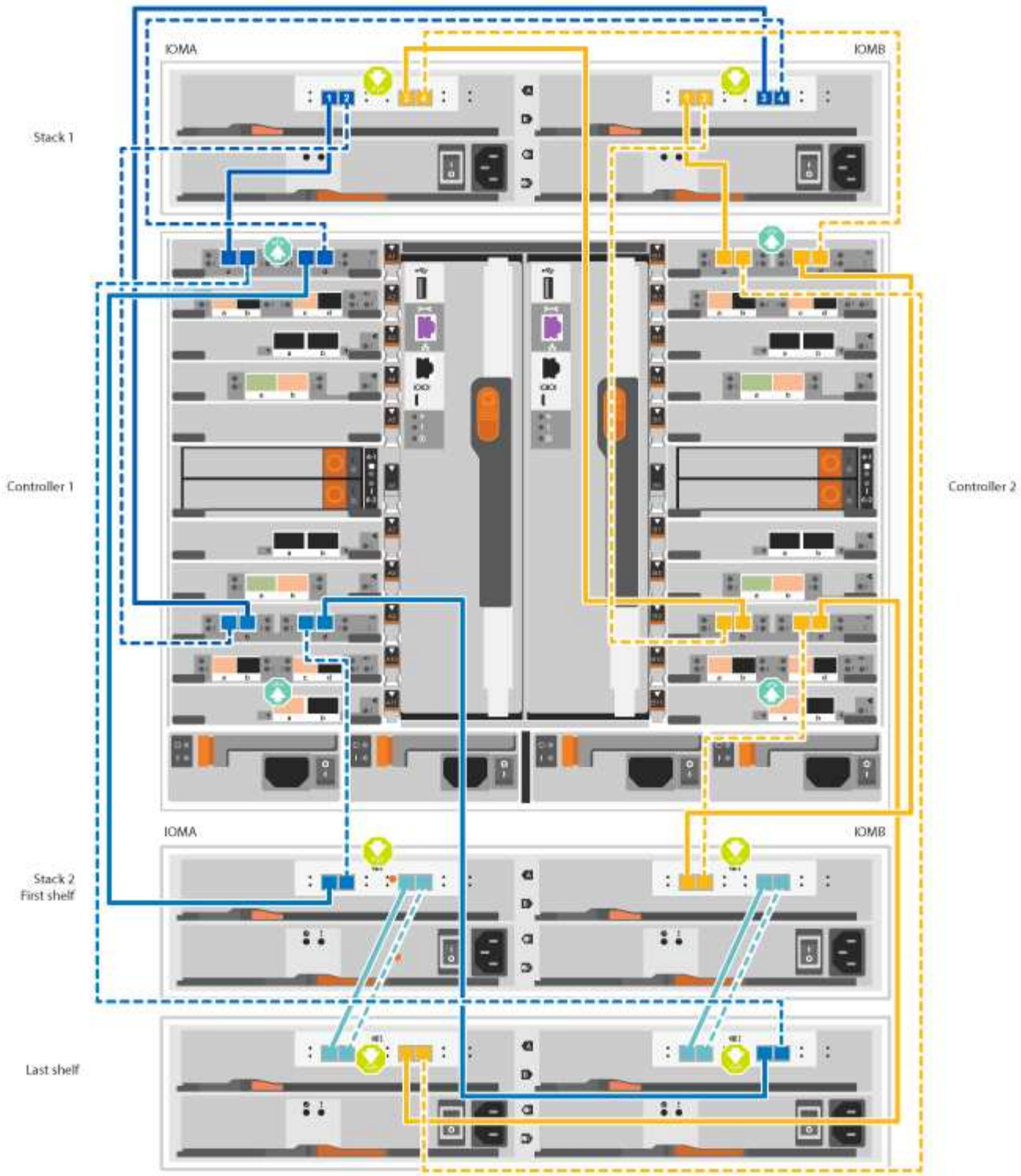
   - Cabling SAS shelves in FAS9000, AFF A700, and ASA AFF A700, ONTAP 9.7 and earlier:

   Cabling SAS storage - ONTAP 9.7 and earlier



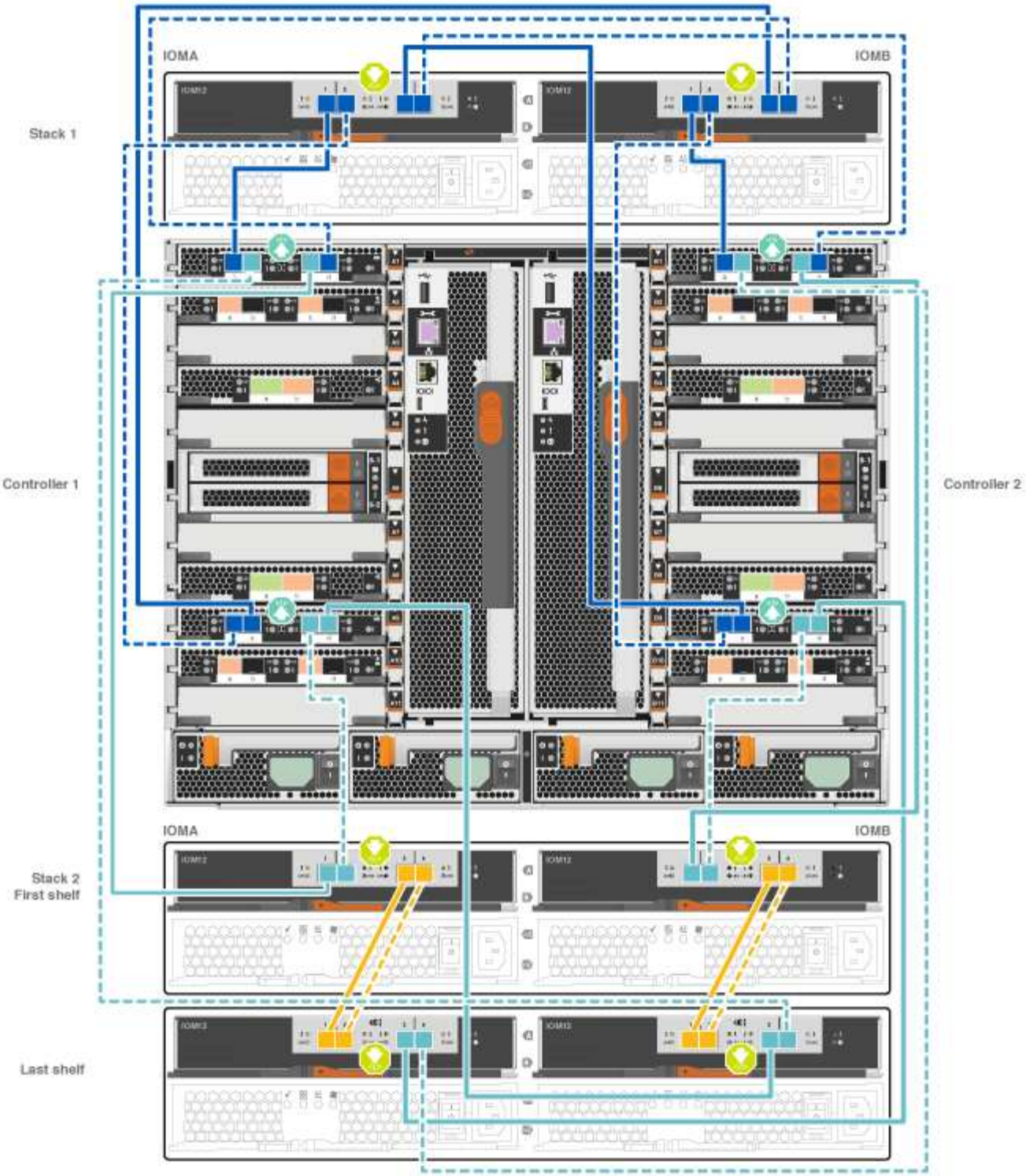

- Cabling SAS shelves in FAS9000, AFF A700, and ASA AFF A700, ONTAP 9.8 and later:

Cabling SAS storage - ONTAP 9.8 and later




If you have more than one drive shelf stack, see the *Installation and Cabling Guide* for your drive shelf type.

Install and cable shelves for a new system installation - shelves with IOM12 modules



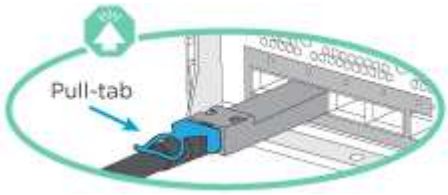

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

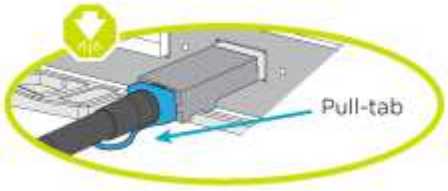
**Option 2: Cable the controllers to a single NS224 drive shelf in AFF A700 and ASA AFF A700 systems running ONTAP 9.8 and later only**

You must cable each controller to the NSM modules on the NS224 drive shelf on an AFF A700 or ASA AFF A700 running system ONTAP 9.8 or later.

- This task applies to AFF A700 and ASA AFF A700 running ONTAP 9.8 or later only.

- The systems must have at least one X91148A module installed in slots 3 and/or 7 for each controller. The animation or illustrations show this module installed in both slots 3 and 7.
- Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the storage modules are up, while the pull tabs on the shelves are down.



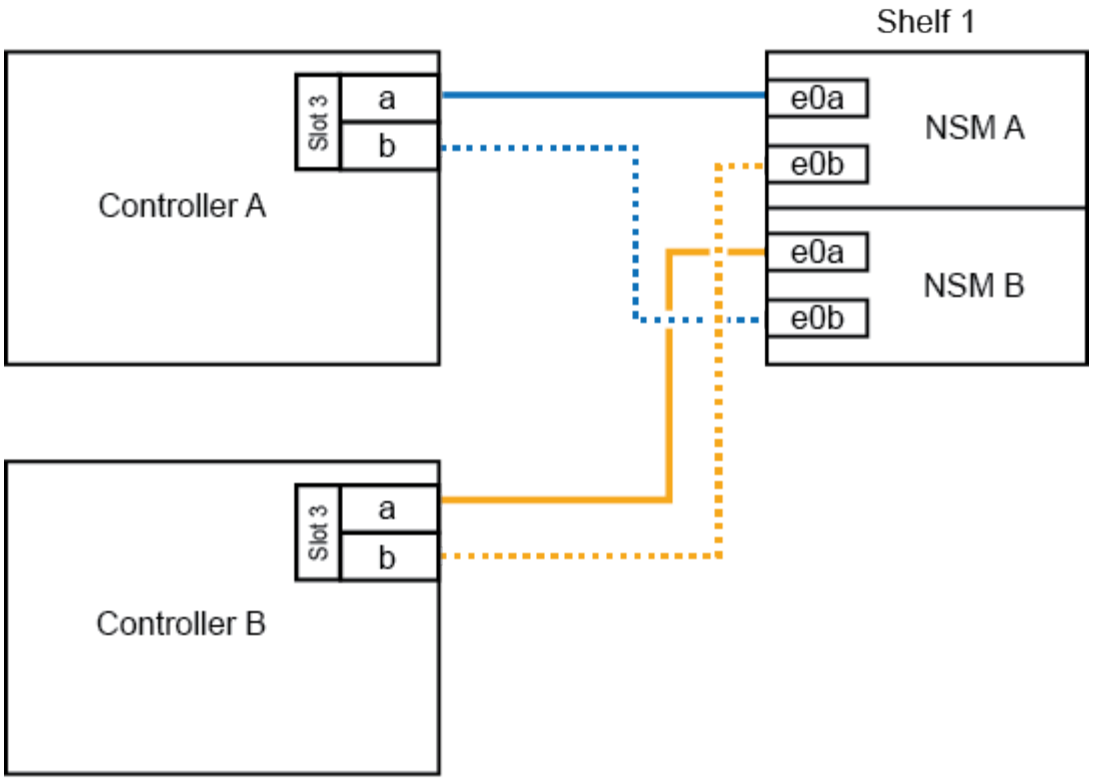

> As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

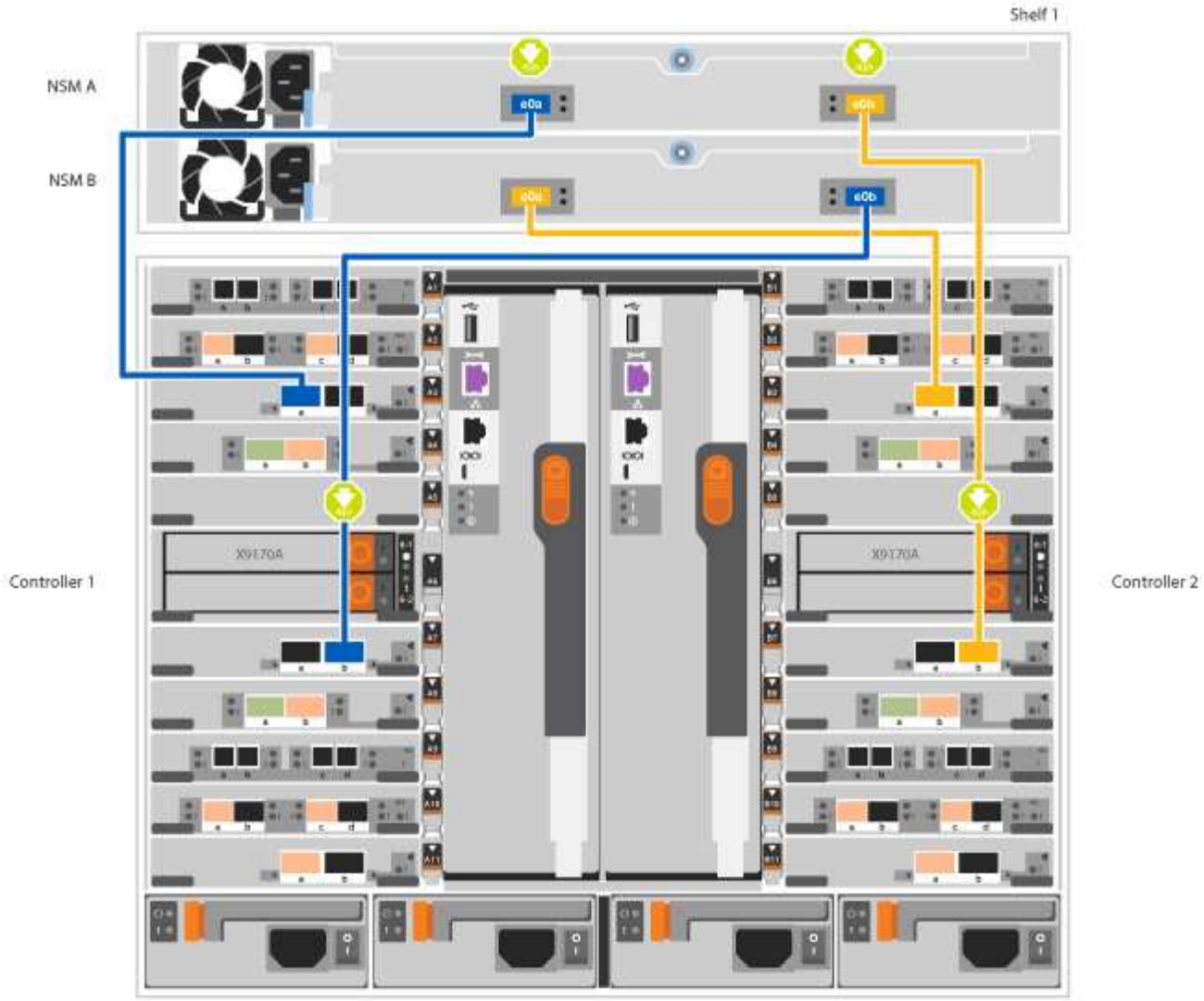
**Steps**

1. Use the following animation or illustrations to cable your controllers with two X91148A storage modules to a single NS224 drive shelf, or use the diagram to cable your controllers with one X91148A storage module to a single NS224 drive shelf.

   Cabling a single NS224 shelf - ONTAP 9.8 and later

AFF A700 or ASA A700 HA pair with one NS224 shelf



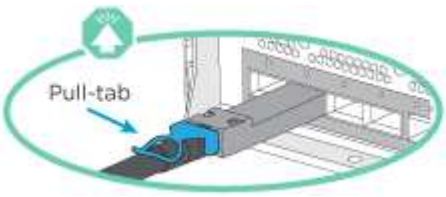


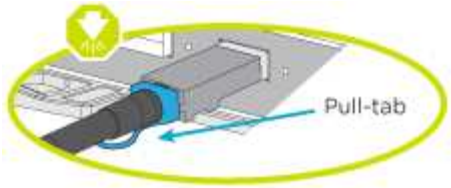

2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

**Option 3: Cable the controllers to two NS224 drive shelves in AFF A700 and ASA AFF A700 systems running ONTAP 9.8 and later only**

You must cable each controller to the NSM modules on the NS224 drive shelves on an AFF A700 or ASA AFF A700 running system ONTAP 9.8 or later.

- This task applies to AFF A700 and ASA AFF A700 running ONTAP 9.8 or later only.
- The systems must have two X91148A modules, per controller, installed in slots 3 and 7.
- Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the storage modules are up, while the pull tabs on the shelves are down.



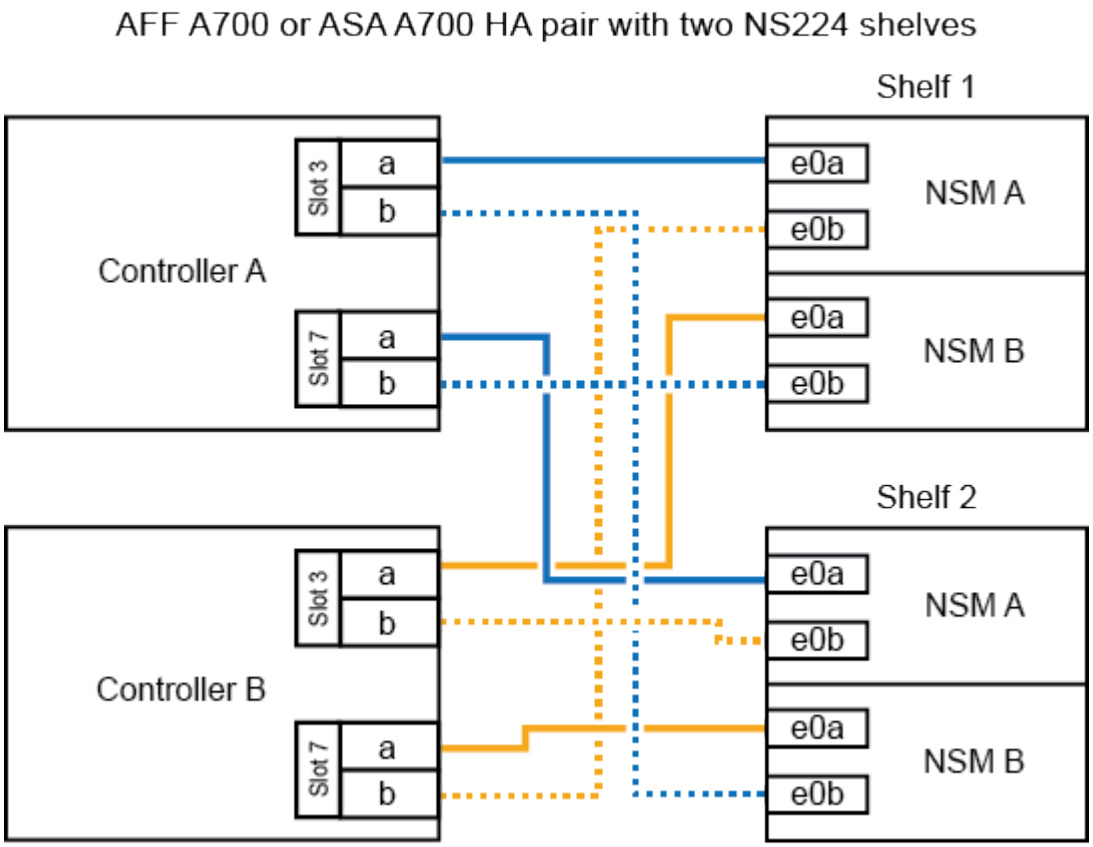


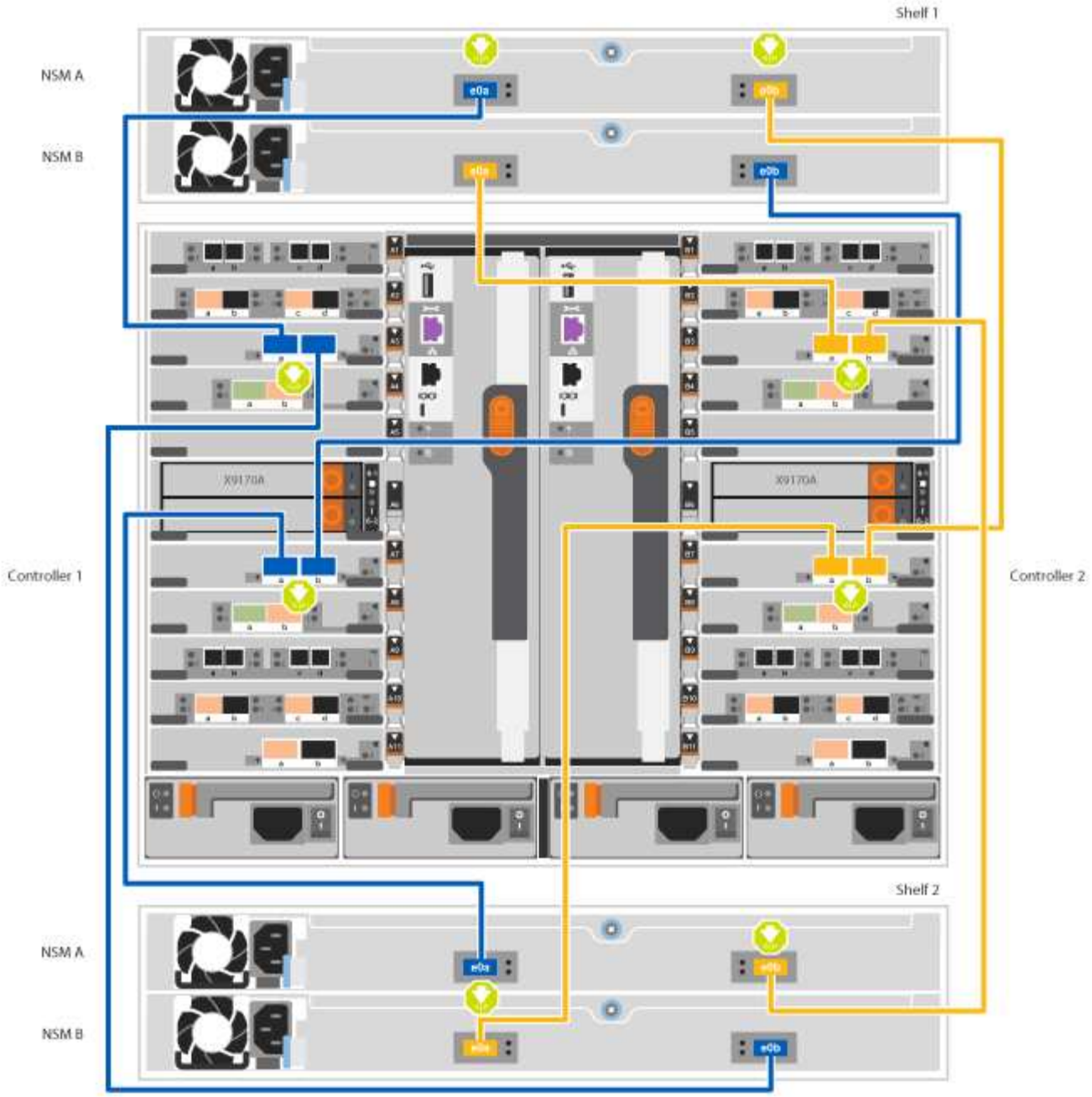

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

**Steps**

1. Use the following animation or illustrations to cable your controllers to two NS224 drive shelves.

   Cabling two NS224 shelves - ONTAP 9.8 and later






2. Go to Step 5: Complete system setup and configuration to complete system setup and configuration.

#### Step 5: Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

#### Option 1: Completing system setup and configuration if network discovery is enabled

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

#### Steps

1. Use the following animation to set one or more drive shelf IDs:

   If your system has NS224 drive shelves, the shelves are pre-set to shelf ID 00 and 01. If you want to change the shelf IDs, you must create a tool to insert into the hole where button is located.

   Setting SAS or NVMe drive shelf IDs

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Turn on the power switches to both nodes.

   Turn on the power to the controllers

   > Initial booting may take up to eight minutes.

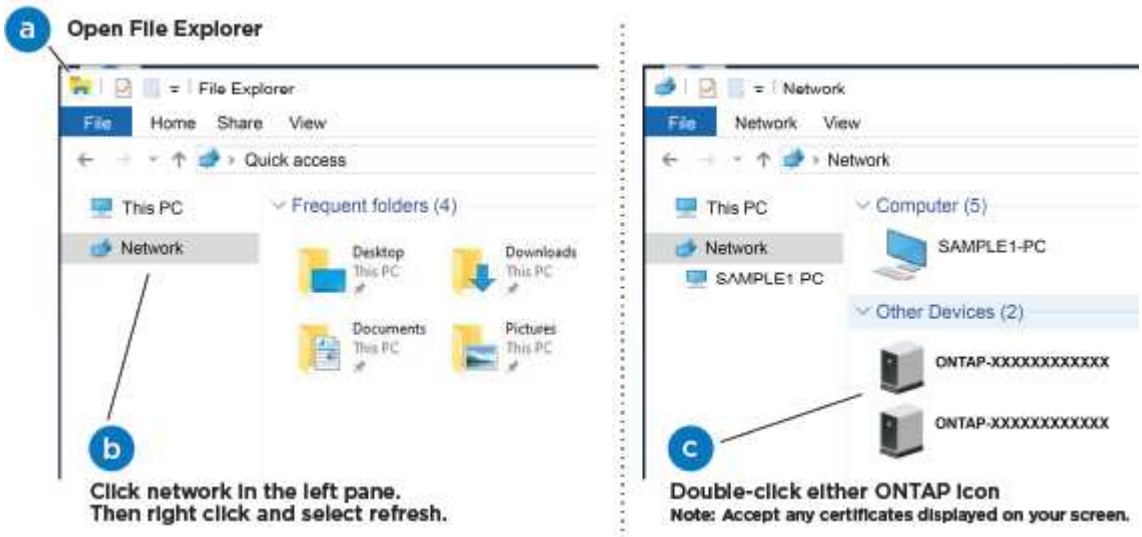
4. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

5. Use the following animation to connect your laptop to the Management switch.

   Connecting your laptop to the Management switch

6. Select an ONTAP icon listed to discover:




   a. Open File Explorer.
   b. Click network in the left pane.
   c. Right click and select refresh.
   d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

      > XXXXX is the system serial number for the target node.

   System Manager opens.

7. Use System Manager guided setup to configure your system using the data you collected in the *NetApp*

*ONTAP Configuration Guide*.

ONTAP Configuration Guide

8. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

   b. Register your system.

      NetApp Product Registration

   c. Download Active IQ Config Advisor.

      NetApp Downloads: Config Advisor

9. Verify the health of your system by running Config Advisor.
10. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

**Option 2: Completing system setup and configuration if network discovery is not enabled**

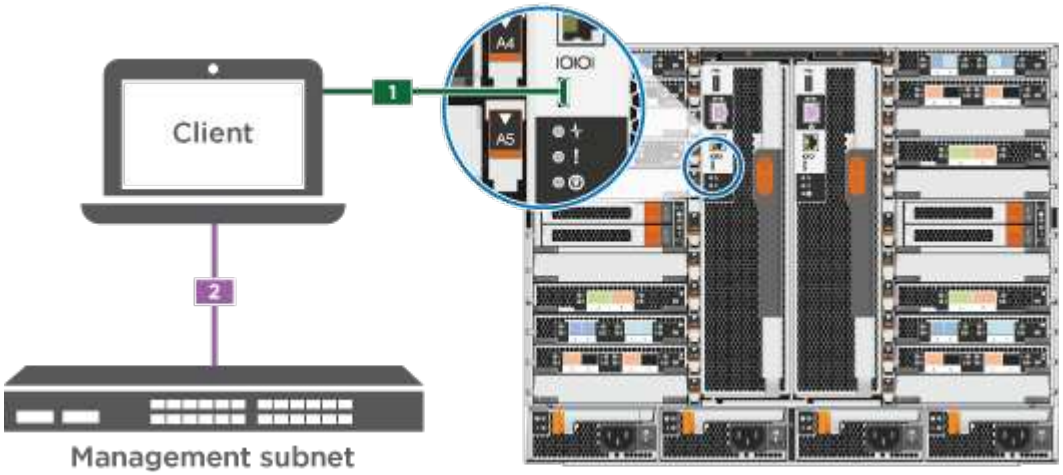
If network discovery is not enabled on your laptop, you must complete the configuration and setup using this task.

**Steps**

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

      See your laptop or console's online help for how to configure the console port.

   b. Connect the console cable to the laptop or console using the console cable that came with your system, and then connect the laptop to the management switch on the management subnet .




   c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.
2. Use the following animation to set one or more drive shelf IDs:

If your system has NS224 drive shelves, the shelves are pre-set to shelf ID 00 and 01. If you want to change the shelf IDs, you must create a tool to insert into the hole where button is located.

Setting SAS or NVMe drive shelf IDs

3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
4. Turn on the power switches to both nodes.

   Turn on the power to the controllers

   Initial booting may take up to eight minutes.

5. Assign an initial node management IP address to one of the nodes.

| If the management network has DHCP… | Then… |
|---|---|
| Configured | Record the IP address assigned to the new controllers. |
| Not configured | a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment.<br>Check your laptop or console's online help if you do not know how to configure PuTTY.<br>b. Enter the management IP address when prompted by the script. |

6. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

      The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the *NetApp ONTAP Configuration guide*.

      ONTAP Configuration Guide

7. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

   b. Register your system.

      NetApp Product Registration

   c. Download Active IQ Config Advisor.

      NetApp Downloads: Config Advisor

8. Verify the health of your system by running Config Advisor.

9. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

## Maintain

### Boot media

#### Overview of boot media replacement - AFF A700 and FAS9000

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 onboard encryption keys

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

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 the NetApp Encryption overview with the CLI.

**Steps**

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.

2. 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`

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.5, go to Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier.
   - If <lno-DARE> is not displayed in the command output, and the system is running ONTAP 9.6 or later, go to Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later.
4. If the impaired node is part of an HA configuration, disable automatic giveback from the healthy node: `storage failover modify -node local -auto-giveback false` or `storage failover modify -node local -auto-giveback-after-panic false`

#### Option 1: Check NVE or NSE on systems running ONTAP 9.5 and earlier

Before shutting down the impaired controller, you need to check whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

**Steps**

1. Connect the console cable to the impaired controller.
2. Check whether NVE is configured for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured.

3. Check whether NSE is configured: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration.
   - If NVE and NSE are not configured, it's safe to shut down the impaired controller.

#### Verify NVE configuration

**Steps**

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled,

you need to complete some other additional steps.

2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:

   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`

   c. Shut down the impaired controller.

3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`

   a. If the `Restored` column displays `yes` manually back up the onboard key management information:

      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.

   b. If the `Restored` column displays anything other than `yes`:

      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column displays `yes` for all authentication key: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - You can safely shutdown the controller.

### Verify NSE configuration

#### Steps

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager query`
   - If the `Restored` column displays `yes` and all key managers display `available`, it's safe to shut down the impaired controller.
   - If the `Restored` column displays anything other than `yes`, or if any key manager displays `unavailable`, you need to complete some additional steps.
   - If you see the message This command is not supported when onboard key management is enabled, you need to complete some other additional steps
2. If the `Restored` column displayed anything other than `yes`, or if any key manager displayed `unavailable`:
   a. Retrieve and restore all authentication keys and associated key IDs: `security key-manager restore -address *`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column displays `yes` for all authentication keys and that all key managers display `available`: `security key-manager query`
   c. Shut down the impaired controller.
3. If you saw the message This command is not supported when onboard key management is enabled, display the keys stored in the onboard key manager: `security key-manager key show -detail`
   a. If the `Restored` column displays `yes`, manually back up the onboard key management information:
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to display the OKM backup information: `security key-manager backup show`
      - Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
      - Return to admin mode: `set -priv admin`
      - Shut down the impaired controller.
   b. If the `Restored` column displays anything other than `yes`:
      - Run the key-manager setup wizard: `security key-manager setup -node target/impaired node name`

        > Enter the customer's OKM passphrase at the prompt. If the passphrase cannot be provided, contact mysupport.netapp.com

      - Verify that the `Restored` column shows `yes` for all authentication keys: `security key-manager key show -detail`
      - Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
      - Enter the command to back up the OKM information: `security key-manager backup show`

> Make sure that OKM information is saved in your log file. This information will be needed in disaster scenarios where OKM might need to be manually recovered.

- Copy the contents of the backup information to a separate file or your log. You'll need it in disaster scenarios where you might need to manually recover OKM.
- Return to admin mode: `set -priv admin`
- You can safely shut down the controller.

**Option 2: Check NVE or NSE on systems running ONTAP 9.6 and later**

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

**Verify NVE configuration**

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

b. Enter the command to display the key management information: `security key-manager onboard show-backup`

c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

d. Return to admin mode: `set -priv admin`

e. Shut down the impaired controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

   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.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

   c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

### Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

> After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
   a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   b. Enter the command to display the key management information: `security key-manager onboard show-backup`
   c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   d. Return to admin mode: `set -priv admin`
   e. You can safely shut down the controller.
2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

#### Shut down the impaired controller - AFF A700 and FAS9000

**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 `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode impaired_node_name`<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

1. 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

**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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### Replace the boot media - AFF A700 and FAS9000

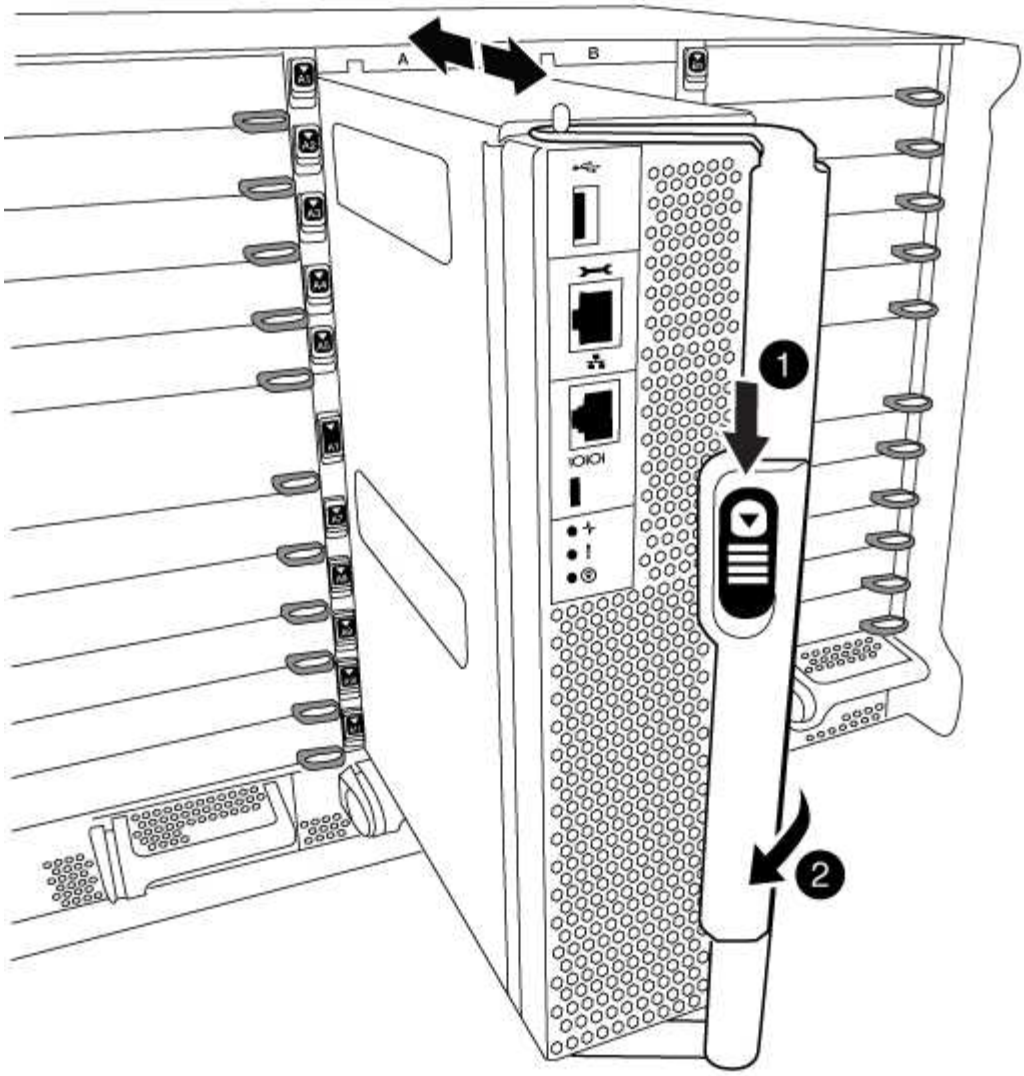
To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

### 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.

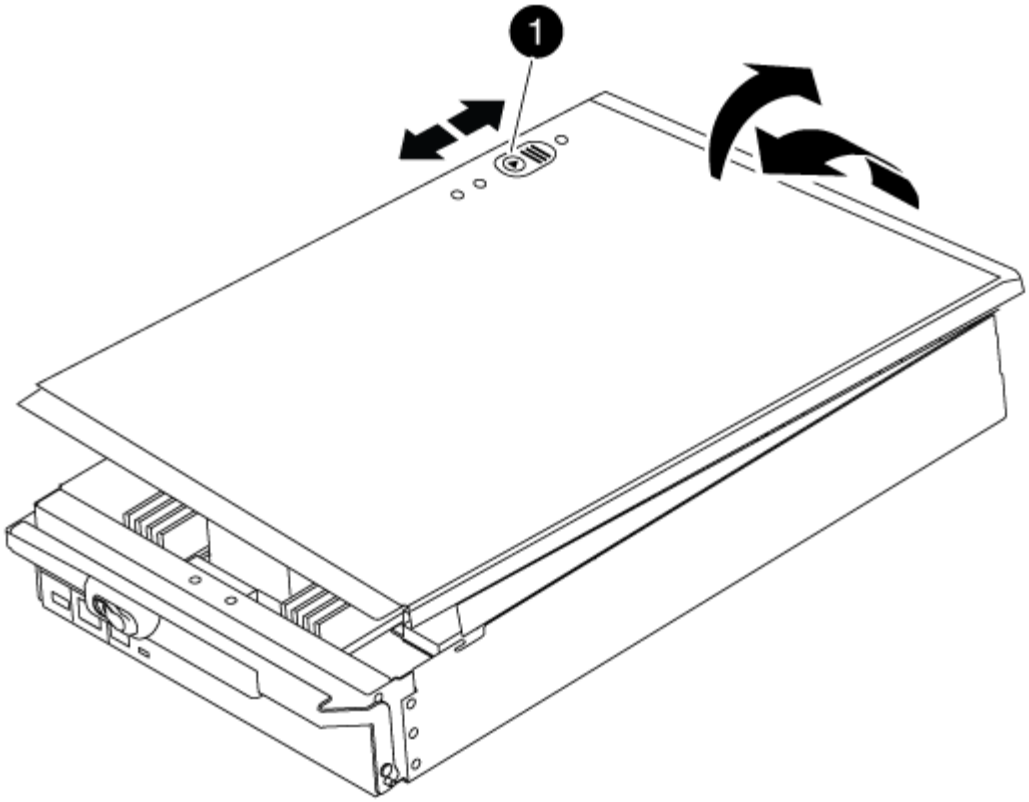



| | |
|---|---|
| 1 | Cam handle release button |
| 2 | Cam handle |

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.

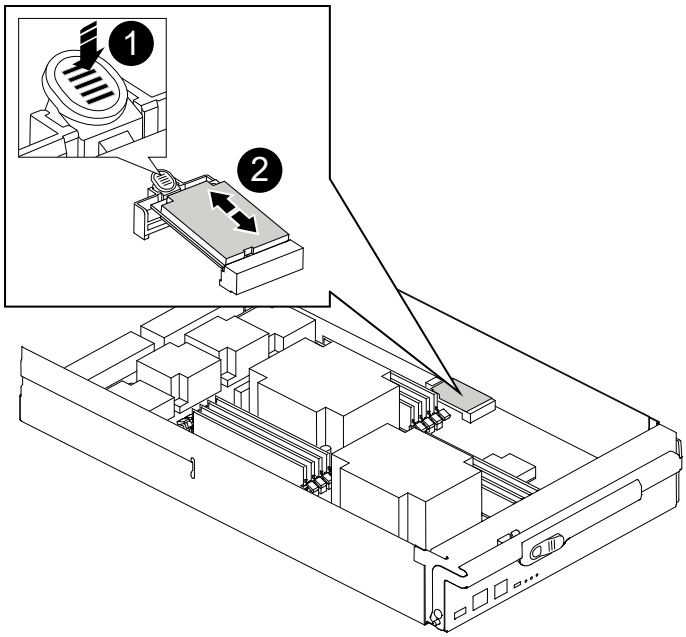
5. Place the controller module lid-side up on a stable, flat surface, press the blue button on the cover, slide the cover to the back of the controller module, and then swing the cover up and lift it off of the controller module.




| | |
|---|---|
| 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:



| | |
|---|---|
| ❶ | Press release tab |
| ❷ | 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 reseat 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 and FAS9000

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

| If your system has… | Then… |
| --- | --- |
| No network connection and is in a MetroCluster IP configuration | a. Press `n` when prompted to restore the backup configuration.<br>b. Reboot the system when prompted by the system.<br>c. Wait for the iSCSI storage connections to connect.<br><br>You can proceed after you see the following messages:<br><br>`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).`<br>`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).`<br>`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).`<br>`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).`<br><br>d. Select the **Update flash from backup config** (sync flash) option from the displayed menu.<br><br>If you are prompted to continue with the update, press `y`. |

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.<br>b. Confirm the target node is ready for giveback with the `storage failover show` 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 and FAS9000

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

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 OKM, NSE, and NVE as needed - AFF A700 and FAS9000

Once environment variables are checked, you must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled.

Determine which section you should use to restore your OKM, NSE, or NVE configurations:

If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.

- If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Option 1: Restore NVE or NSE when Onboard Key Manager is enabled.
- If NSE or NVE are enabled for ONATP 9.5, go to Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier.
- If NSE or NVE are enabled for ONTAP 9.6, go to Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later.

### Option 1: Restore NVE or NSE when Onboard Key Manager is enabled

**Steps**

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
| --- | --- |
| The LOADER prompt | Boot the controller to the boot menu: `boot_ontap menu` |
| Waiting for giveback… | a. Enter `Ctrl-C` at the prompt<br>b. At the message: Do you wish to halt this controller rather than wait [y/n]? , enter: `y`<br>c. At the LOADER prompt, enter the `boot_ontap menu` command. |

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager` and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this procedure, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

   The data is output from either `security key-manager backup show` or `security key-manager onboard show-backup` command.

   Example of backup data:


```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to `Waiting for giveback…` prompt.

8. Move the console cable to the partner controller and login as admin.

9. Confirm the target controller is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the storage failover giveback `-fromnode local -only-cfo -aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

      Terminating CIFS can cause loss of data.

    - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `` `storage failover show`-giveback` `` commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.
12. Move the console cable to the target controller.
13. If you are running ONTAP 9.5 and earlier, run the key-manager setup wizard:
    a. Start the wizard using the `security key-manager setup -nodenodename` command, and then enter the passphrase for onboard key management when prompted.
    b. Enter the `key-manager key show -detail` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
14. If you are running ONTAP 9.6 or later:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.

       If the `Restored` column = anything other than `yes/true`, contact Customer Support.

    c. Wait 10 minutes for the key to synchronize across the cluster.
15. Move the console cable to the partner controller.
16. Give back the target controller using the `storage failover giveback -fromnode local` command.
17. Check the giveback status, 3 minutes after it reports complete, using the `storage failover show` command.

If giveback is not complete after 20 minutes, contact Customer Support.

18. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

19. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
20. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

### Option 2: Restore NSE/NVE on systems running ONTAP 9.5 and earlier

**Steps**

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
|---|---|
| The login prompt | Go to Step 7. |
| Waiting for giveback… | a. Log into the partner controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

`revert` command.

7. Move the console cable to the target controller and run the version `-v command` to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.

   This command does not work if NVE (NetApp Volume Encryption) is configured

10. Use the security key-manager query to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes` and all key managers report in an available state, go to *Complete the replacement process*.
    - If the `Restored` column = anything other than `yes`, and/or one or more key managers is not available, use the `security key-manager restore -address` command to retrieve and restore all authentication keys (AKs) and key IDs associated with all nodes from all available key management servers.

      Check the output of the security key-manager query again to ensure that the `Restored` column = `yes` and all key managers report in an available state

11. If the Onboard Key Management is enabled:
    a. Use the `security key-manager key show -detail` to see a detailed view of all keys stored in the onboard key manager.
    b. Use the `security key-manager key show -detail` command and verify that the `Restored` column = `yes` for all authentication keys.

       If the `Restored` column = anything other than `yes`, use the `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* command to restore the Onboard Key Management settings. Rerun the `security key-manager key show -detail` command to verify `Restored` column = `yes` for all authentication keys.

12. Connect the console cable to the partner controller.
13. Give back the controller using the `storage failover giveback -fromnode local` command.
14. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

### Option 3: Restore NSE/NVE on systems running ONTAP 9.6 and later

#### Steps

1. Connect the console cable to the target controller.
2. Use the `boot_ontap` command at the LOADER prompt to boot the controller.
3. Check the console output:

| If the console displays… | Then… |
| --- | --- |
| The login prompt | Go to Step 7. |
| Waiting for giveback… | a. Log into the partner controller.<br>b. Confirm the target controller is ready for giveback with the `storage failover show` command. |

4. Move the console cable to the partner controller and give back the target controller storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS session, check with the customer on how to close out CIFS sessions.

     Terminating CIFS can cause loss of data.

   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to synchronize.
   - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate Documentation Center for more information.
5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home controller and port.

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

7. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key query` command to display the key IDs of the authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

- If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

  Use the security key-manager key query to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner controller.
12. Give back the controller using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

#### Return the failed part to NetApp - AFF A700 and FAS9000

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Replace the caching module or add/replace a core dump module - AFF A700 and FAS9000

You must replace the caching module in the controller module when your system registers a single AutoSupport (ASUP) message that the module has gone offline; failure to do so results in performance degradation. If AutoSupport is not enabled, you can locate the failed caching module by the fault LED on the front of the module. You can also add or replace the 1TB, X9170A core dump module, which is required if you are installing NS224 drive shelves in an AFF A700 system.

#### Before you begin

- You must replace the failed component with a replacement FRU component you received from your provider.
- For instructions about hot swapping the caching module, see Hot-swapping a caching module.
- When removing, replacing, or adding caching or core dump modules, the target node must be halted to the LOADER.
- AFF A700 supports the 1TB core dump module, X9170A, which is required if you are adding NS224 drive shelves.
- The core dump modules can be installed in slots 6-1 and 6-2. The recommended best practice is to install the module in slot 6-1.
- The X9170A core dump module is not hot-swappable.

#### Step 1: Shutting down the impaired controller

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

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

**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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

#### Step 2: Replace or add a caching module

The NVMe SSD Flash Cache modules (FlashCache or caching modules) are separate modules. They are located in the front of the NVRAM module. To replace or add a caching module, locate it on the rear of the system on slot 6, and then follow the specific sequence of steps to replace it.

**Before you begin**

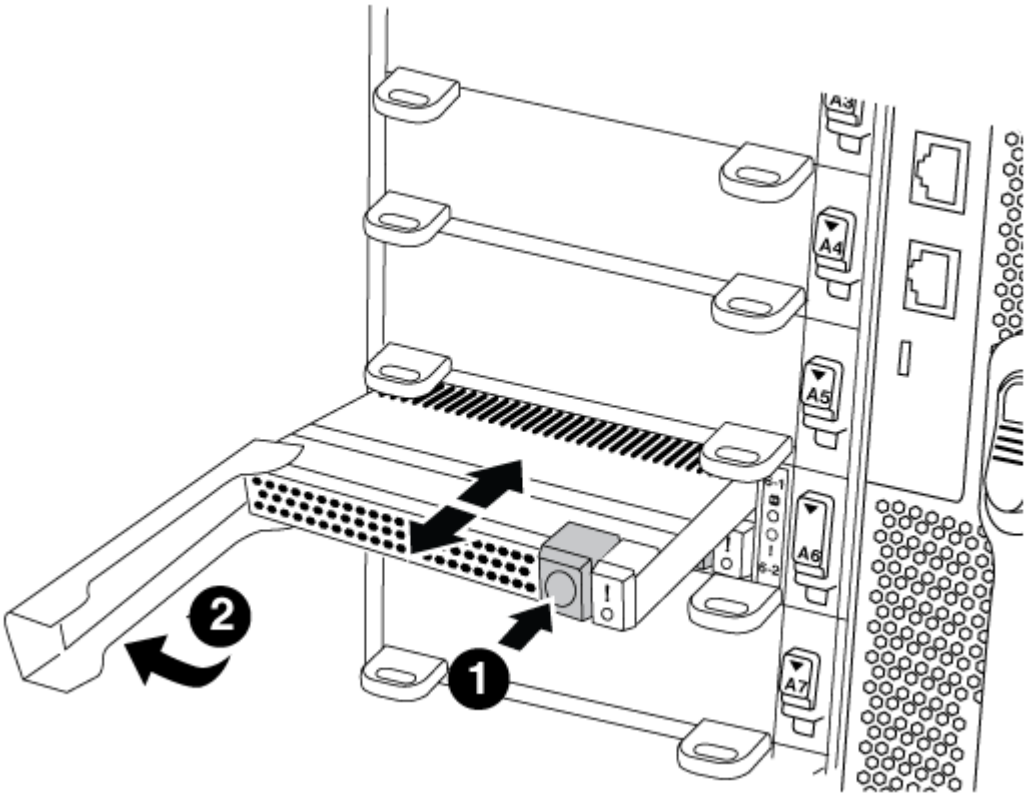
Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- The target node must be at the LOADER prompt before adding or replacing the caching module.
- The replacement caching module must have the same capacity as the failed caching module, but can be from a different supported vendor.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

**Steps**

1. If you are not already grounded, properly ground yourself.
2. Locate the failed caching module, in slot 6, by the lit amber Attention LED on the front of the caching module.
3. Remove the caching module:

> If you are adding another caching module to your system, remove the blank module and go to the next step.



| | |
|---|---|
| 1 | Orange release button. |
| 2 | Caching module cam handle. |

a. Press the orange release button on the front of the caching module.

> Do not use the numbered and lettered I/O cam latch to eject the caching module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the caching module.

b. Rotate the cam handle until the caching module begins to slide out of the NVRAM10 module.

c. Gently pull the cam handle straight toward you to remove the caching module from the NVRAM10 module.

   Be sure to support the caching module as you remove it from the NVRAM10 module.

4. Install the caching module:

   a. Align the edges of the caching module with the opening in the NVRAM10 module.

   b. Gently push the caching module into the bay until the cam handle engages.

   c. Rotate the cam handle until it locks into place.

#### Step 3: Add or replace an X9170A core dump module

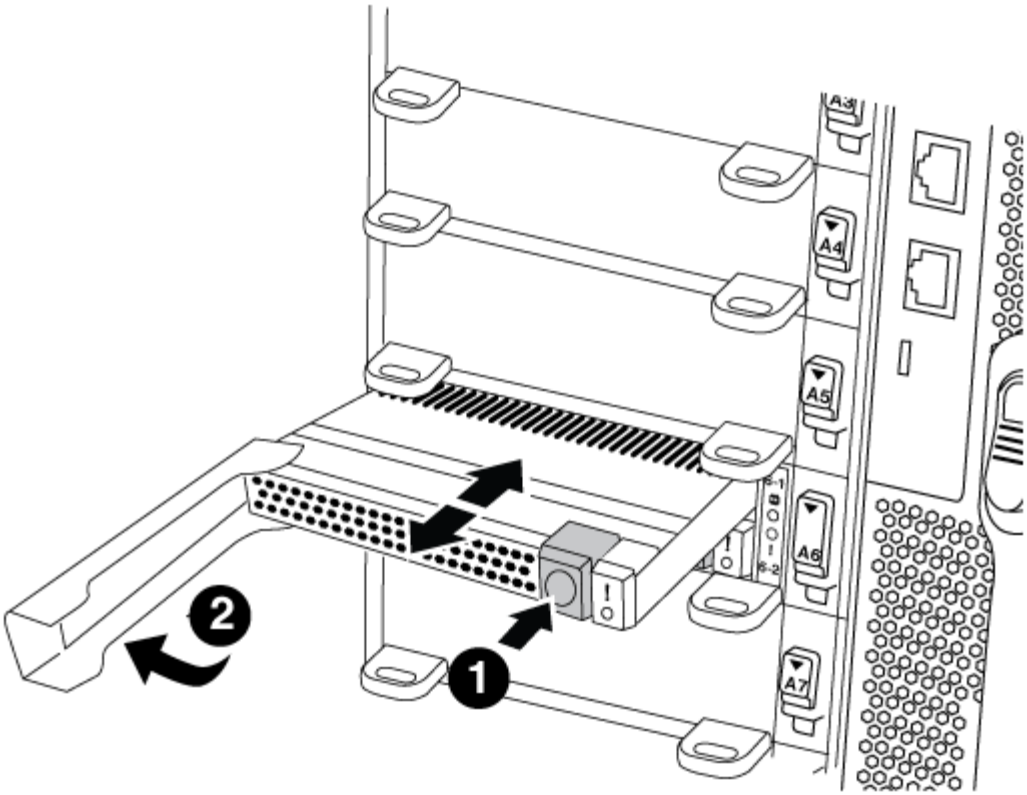
The 1TB cache core dump, X9170A, is only used in the AFF A700 systems. The core dump module cannot be hot-swapped. The core dump module typically is located in the front of the NVRAM module in slot 6-1 in the rear of the system. To replace or add the core dump module, locate slot 6-1, and then follow the specific sequence of steps to add or replace it.

**Before you begin**

- Your system must be running ONTAP 9.8 or later in order to add a core dump module.
- The X9170A core dump module is not hot-swappable.
- The target node must be at the LOADER prompt before adding or replacing the code dump module.
- You must have received two X9170 core dump modules; one for each controller.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

**Steps**

1. If you are not already grounded, properly ground yourself.
2. If you are replacing a failed core dump module, locate and remove it:




| | |
|---|---|
| 1 | Orange release button. |
| 2 | Core dump module cam handle. |

a. Locate the failed module by the amber Attention LED on the front of the module.
b. Press the orange release button on the front of the core dump module.

> Do not use the numbered and lettered I/O cam latch to eject the core dump module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the core dump module.

c. Rotate the cam handle until the core dump module begins to slide out of the NVRAM10 module.
d. Gently pull the cam handle straight toward you to remove the core dump module from the NVRAM10 module and set it aside.

   Be sure to support the core dump module as you remove it from the NVRAM10 module.

3. Install the core dump module:
   a. If you are installing a new core dump module, remove the blank module from slot 6-1.
   b. Align the edges of the core dump module with the opening in the NVRAM10 module.
   c. Gently push the core dump module into the bay until the cam handle engages.
   d. Rotate the cam handle until it locks into 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: Switch back aggregates in a two-node MetroCluster configuration

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

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 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 & Replacements page for further information.

### Hot-swap a caching module - AFF A700 and FAS9000

The NVMe SSD FlashCache modules (FlashCache or caching modules) are located in the front of the NVRAM10 module in Slot 6 of FAS9000 systems only. Beginning with ONTAP 9.4, you can hot-swap the caching module of the same capacity from the same or different supported vendor.

#### Before you begin

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- It must support the caching capacity.
- The replacement caching module must have the same capacity as the failed caching module, but can be from a different supported vendor.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

#### Steps

1. If you are not already grounded, properly ground yourself.
2. Locate the failed caching module, in slot 6, by the lit amber Attention LED on the front of the caching module.

3. Prepare the caching module slot for replacement as follows:

   a. For ONTAP 9.7 and earlier:

      i. Record the caching module capacity, part number, and serial number on the target node: `system node run local sysconfig -av 6`

      ii. In admin privilege level, prepare the target NVMe slot for replacement, responding `y` when prompted whether to continue: `system controller slot module replace -node node_name -slot slot_number` The following command prepares slot 6-2 on node1 for replacement, and displays a message that it is safe to replace:

```
::> system controller slot module replace -node node1 -slot 6-2

Warning: NVMe module in slot 6-2 of the node node1 will be powered
off for replacement.
Do you want to continue? (y|n): `y`

The module has been successfully powered off.  It can now be
safely replaced.
After the replacement module is inserted, use the "system
controller slot module insert" command to place the module into
service.
```

      iii. Display the slot status with the system controller slot module show command.

      The NVMe slot status displays waiting-for-replacement in the screen output for the caching module that needs replacing.

   b. For ONTAP 9.8 and later:

      i. Record the caching module capacity, part number, and serial number on the target node: `system node run local sysconfig -av 6`

      ii. In admin privilege level, prepare the target NVMe slot for removal, responding `y` when prompted whether to continue: `system controller slot module remove -node node_name -slot slot_number` The following command prepares slot 6-2 on node1 for removal, and displays a message that it is safe to remove:

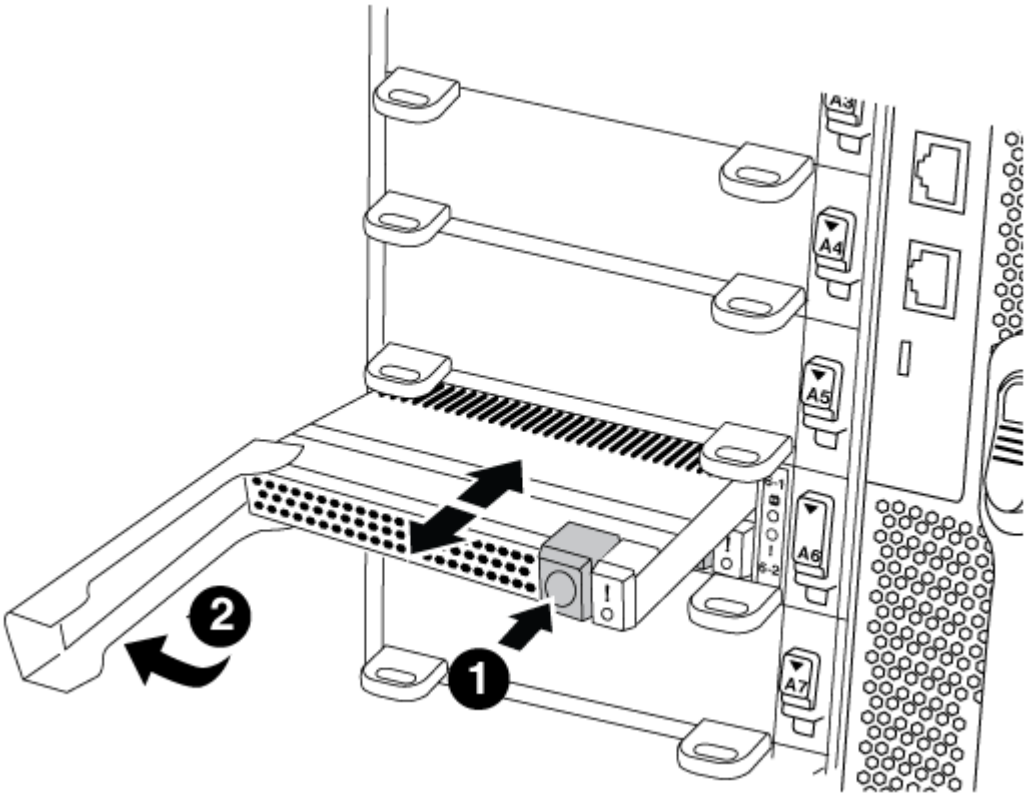
```
::> system controller slot module remove -node node1 -slot 6-2

Warning: SSD module in slot 6-2 of the node node1 will be powered
off for removal.
Do you want to continue? (y|n): `y`

The module has been successfully removed from service and powered
off. It can now be safely removed.
```

      iii. Display the slot status with the `system controller slot module show` command.

The NVMe slot status displays `powered-off` in the screen output for the caching module that needs replacing.

> See the Command man pages for your version of ONTAP for more details.

4. Remove the caching module:




| | |
|---|---|
| 1 | Orange release button. |
| 2 | Caching module cam handle. |

a. Press the orange release button on the front of the caching module.

> Do not use the numbered and lettered I/O cam latch to eject the caching module. The numbered and lettered I/O cam latch ejects the entire NVRAM10 module and not the caching module.

b. Rotate the cam handle until the caching module begins to slide out of the NVRAM10 module.

c. Gently pull the cam handle straight toward you to remove the caching module from the NVRAM10 module.

   Be sure to support the caching module as you remove it from the NVRAM10 module.

5. Install the caching module:

a. Align the edges of the caching module with the opening in the NVRAM10 module.

b. Gently push the caching module into the bay until the cam handle engages.

c. Rotate the cam handle until it locks into place.

6. Bring the replacement caching module online by using the `system controller slot module insert` command as follows:

   The following command prepares slot 6-2 on node1 for power-on, and displays a message that it is powered on:

```
::> system controller slot module insert -node node1 -slot 6-2

Warning: NVMe module in slot 6-2 of the node localhost will be powered
on and initialized.
Do you want to continue? (y|n): `y`

The module has been successfully powered on, initialized and placed into
service.
```

7. Verify the slot status using the `system controller slot module show` command.

   Make sure that command output reports status for slot 6-1 or 6-2 as `powered-on` and ready for operation.

8. Verify that the replacement caching module is online and recognized, and then visually confirm that the amber attention LED is not lit: `sysconfig -av slot_number`

   > If you replace the caching module with a caching module from a different vendor, the new vendor name is displayed in the command output.

9. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

## Chassis

### Overview of chassis replacement - AFF A700 and FAS9000

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 and FAS9000

To replace the chassis, you must shutdown the controllers.

#### Option 1: Shut down the controllers

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

**About this task**

- If you have a cluster with more than two controllers, 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 the Administration overview with the CLI.
- 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`

**Steps**

1. If your system has two controller modules, disable the HA pair.

| If your system is running clustered ONTAP with… | Then… |
|---|---|
| Two controllers in the cluster | `cluster ha modify -configured false` `storage failover modify -node node0 -enabled false` |
| More than two controllers in the cluster | `storage failover modify -node node0 -enabled false` |

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true`

`-skip-lif-migration-before-shutdown true`

Answer `y` when prompted.

### 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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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 and FAS9000

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.

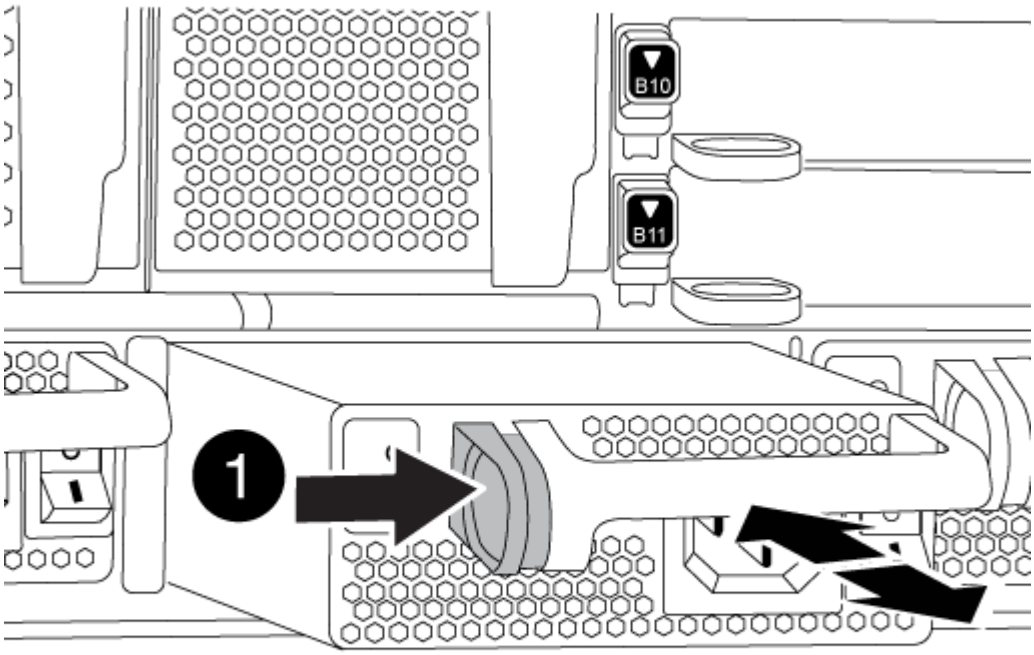
### Step 1: Remove the power supplies

#### 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.

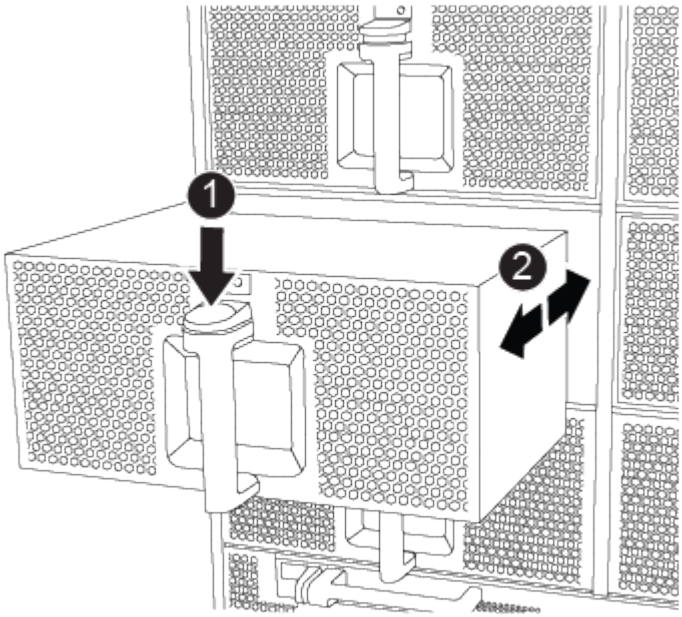
### Step 2: Remove the fans

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 |

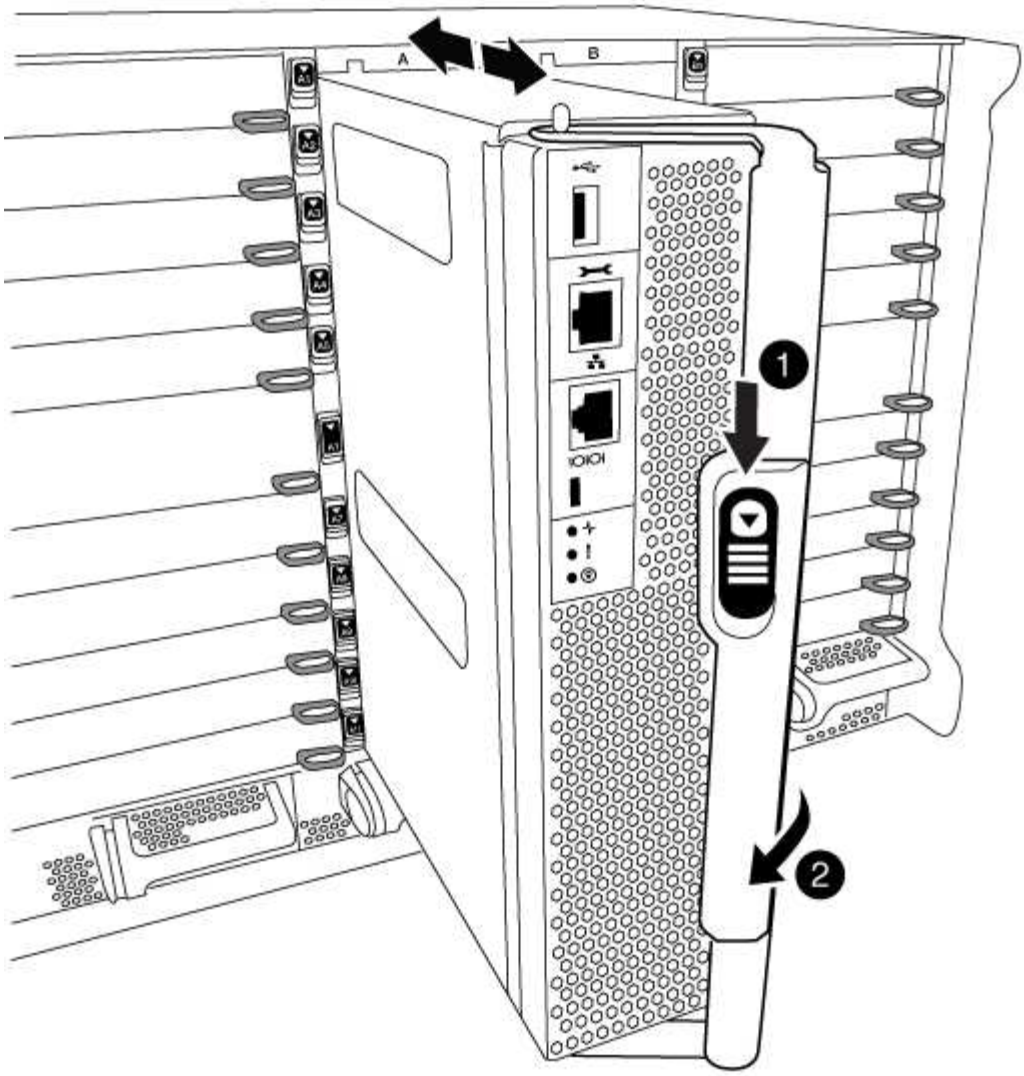
3. Set the fan module aside.
4. Repeat the preceding steps for any remaining fan modules.

### 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 FlashCache 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.

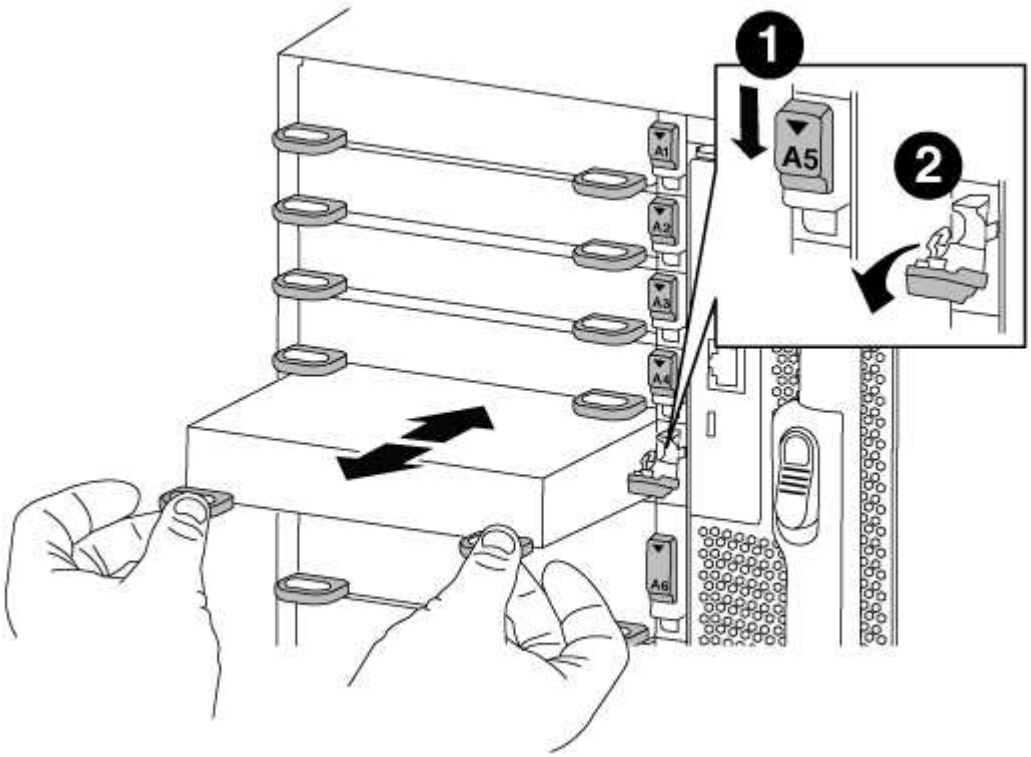
      The cam button moves away from the chassis.

   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 |

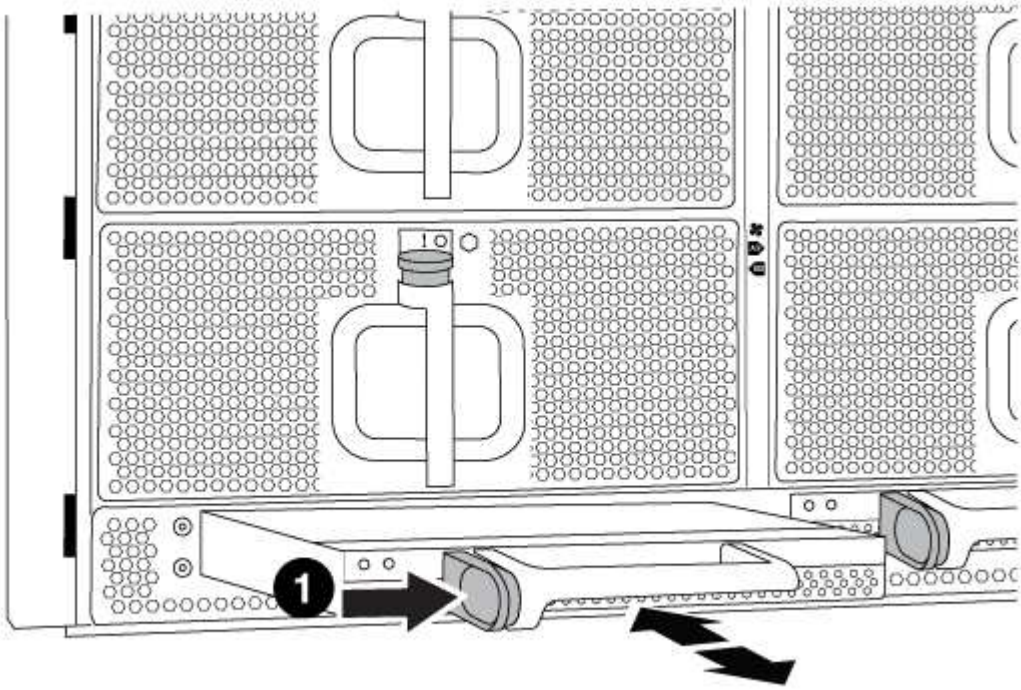
3. Set the I/O module aside.
4. Repeat the preceding step for the remaining I/O modules in the old chassis.

### 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/FlashCache 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 to a state where you can run the interconnect diagnostic test.

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 and FAS9000

## You must verify the HA state of the chassis, run diagnostics, 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: Running system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

**Steps**

1. If the node to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the node boots to Maintenance mode, halt the node: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second node if you are in an HA configuration.

   Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

| If the system-level diagnostics tests… | Then… |
| --- | --- |
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br><br>The following default response is displayed:<br><br>`SLDIAG: No log messages are present.`<br><br>c. Exit Maintenance mode on both controllers: `halt`<br><br>The system displays the LOADER prompt.<br><br>You must exit Maintenance mode on both controllers before proceeding any further.<br><br>d. Enter the following command on both controllers at the LOADER prompt: `bye`<br>e. Return the node to normal operation: |
| With two nodes in the cluster | Issue these commands: `node::> cluster ha modify -configured true`<br><br>`node::> storage failover modify -node node0 -enabled true` |
| With more than two nodes in the cluster | Issue this command:`node::> storage failover modify -node node0 -enabled true` |
| In a two-node MetroCluster configuration | Proceed to the next step.<br><br>The MetroCluster switchback procedure is done in the next task in the replacement process. |
| In a stand-alone configuration | You have no further steps in this particular task.<br><br>You have completed system-level diagnostics. |

| If the system-level diagnostics tests… | Then… |
| --- | --- |
| Resulted in some test failures | Determine the cause of the problem.<br>a. Exit Maintenance mode: `halt`<br>b. Perform a clean shutdown, and then disconnect the power supplies.<br>c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Reconnect the power supplies, and then power on the storage system.<br>e. Rerun the system-level diagnostics test. |

### Step 3: Switch back aggregates in a two-node MetroCluster configuration

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

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 & Replacements page for further information.

### Controller module

#### Overview of controller module replacement - AFF A700 and FAS9000

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 is a FlexArray system or 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

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

**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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

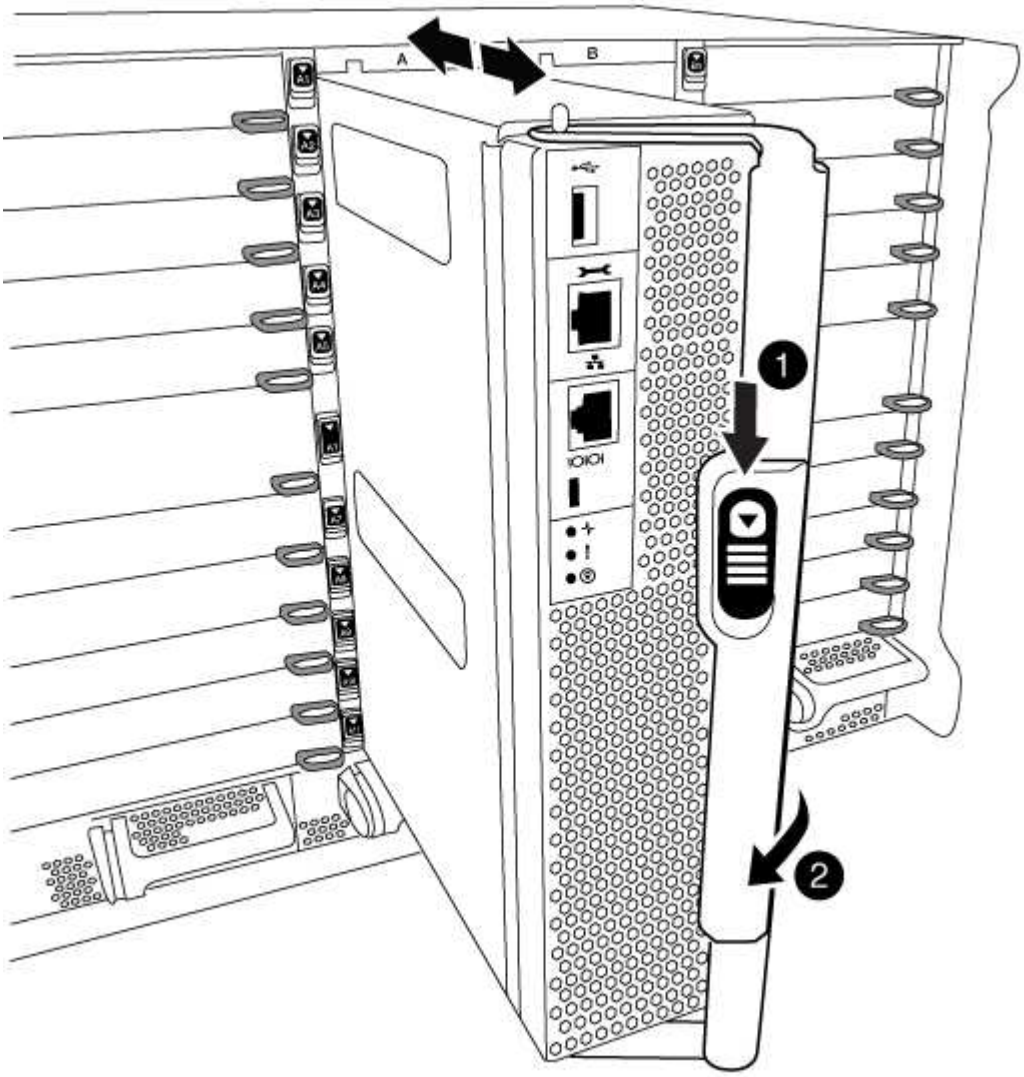
To replace the controller module hardware, you must remove the impaired node, move FRU components to the replacement controller module, install the replacement controller module in the chassis, and then boot the system to Maintenance mode.

### 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.

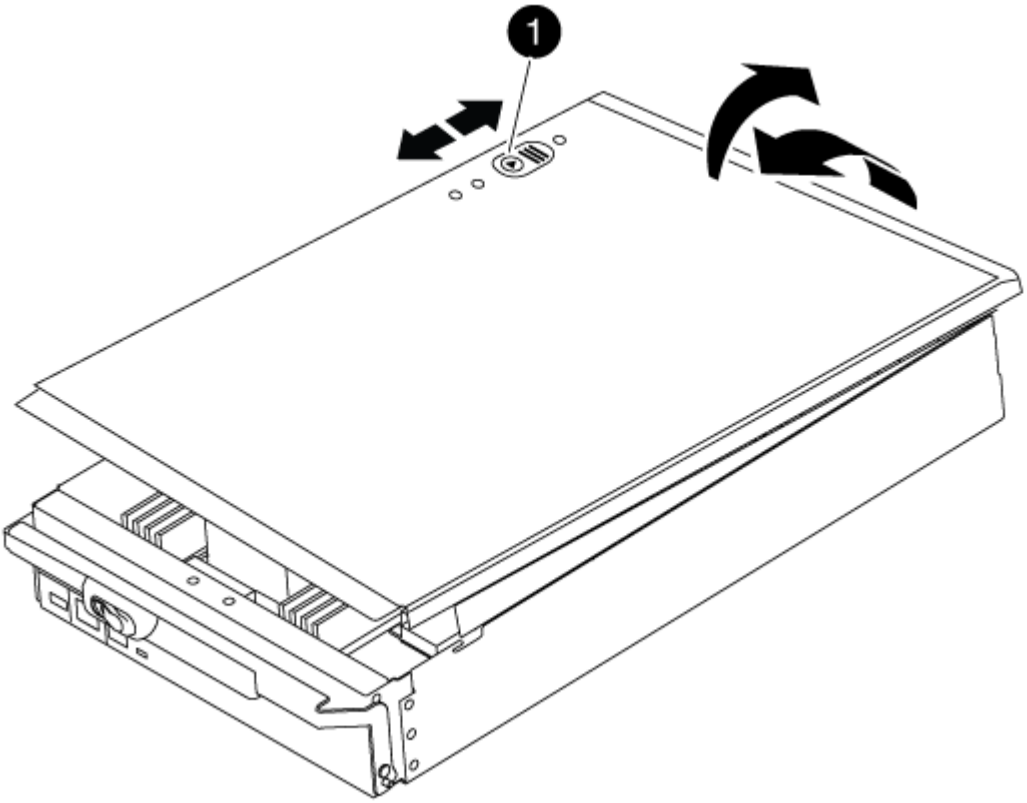


| |
|---|
| ❶ |
| Cam handle release button |
| ❷ |
| Cam handle |

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.



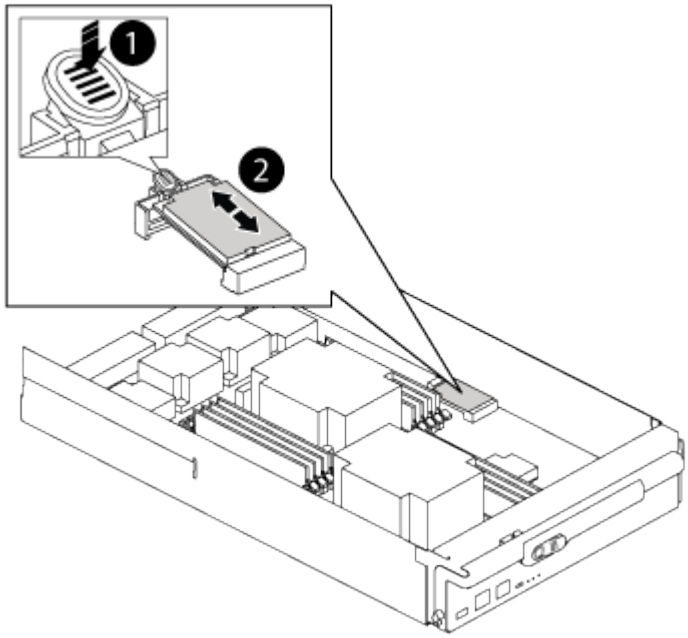

| |
|---|
| ❶ |
| Controller module cover locking button |

### 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 reseat it into the socket.

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

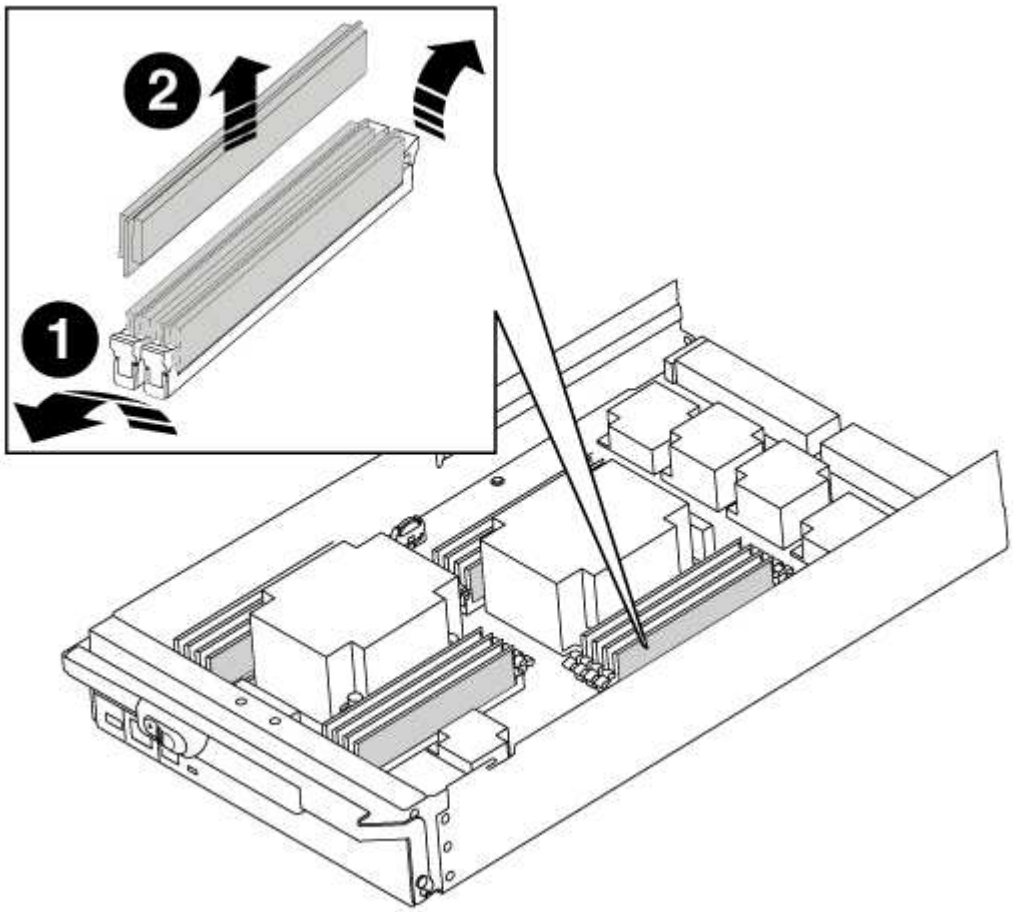
### Step 3: Move the system DIMMs

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 |

| | |
|---|---|
| ❷ | |
| 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 and FAS9000

## 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 after replacing the controller

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

#### About this task

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

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

#### Steps

1. 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: `show date`

   The date and time are given in GMT.

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 HA state of the controller module

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

#### Steps

1. In Maintenance mode from the new controller module, verify that all components display the same `HA` state: `ha-config show`

   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`

### Step 3: Run system-level diagnostics

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

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

#### Steps

1. If the node to be serviced is not at the LOADER prompt, reboot the node: `halt`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

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

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

   - `bootmedia` is the system booting device.
   - `cna` is a Converged Network Adapter or interface not connected to a network or storage device.
   - `fcal` is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
   - `env` is motherboard environmentals.
   - `mem` is system memory.

- `nic` is a network interface card.
- `nvram` is nonvolatile RAM.
- `nvmem` is a hybrid of NVRAM and system memory.
- `sas` is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

| If you want to run diagnostic tests on… | Then… |
|---|---|
| Individual components | a. Clear the status logs: `sldiag device clearstatus`<br>b. Display the available tests for the selected devices: `sldiag device show -dev _dev_name`<br><br>`dev_name` can be any one of the ports and devices identified in the preceding step.<br><br>c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only`<br>+<br>`-selection only` disables all other tests that you do not want to run for the device.<br>d. Run the selected tests: `sldiag device run -dev dev_name`<br><br>After the test is complete, the following message is displayed:<br><br>`*> <SLDIAG:_ALL_TESTS_COMPLETED>`<br><br>e. Verify that no tests failed: `sldiag device status -dev dev_name -long -state failed`<br><br>System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component. |

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

5. Proceed based on the result of the preceding step:

| If the system-level diagnostics tests… | Then… |
| --- | --- |
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>`SLDIAG: No log messages are present.`<br>c. Exit Maintenance mode: `halt`<br>The node displays the LOADER prompt.<br>d. Boot the node from the LOADER prompt: `bye`<br>e. Return the node to normal operation: |
| An HA pair | Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`*<br>If you disabled automatic giveback, re-enable it with the `storage failover modify` command. |
| A two-node MetroCluster configuration | Proceed to the next step.<br>The MetroCluster switchback procedure is done in the next task in the replacement process. |
| A stand-alone configuration | Proceed to the next step.<br>No action is required.<br>You have completed system-level diagnostics. |

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

#### Recable the system and reassign disks - AFF A700 and FAS9000

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

#### Step 1: Recable the system

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

#### Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

**Step 2: Reassign disks**

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. 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`
                                      Takeover
Node               Partner            Possible     State Description
------------       ------------       --------
-------------------------------------
node1              node2              false        System ID changed on
partner (Old:
                                                     151759755, New:
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 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

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`

#### Complete system restoration - AFF A700 and FAS9000

## 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.

#### 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.

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

   NetApp Support

   > 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.

**Steps**

1. Install each license key: `system license add -license-code license-key, license-key...`
2. 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: Restoring Storage and Volume Encryption functionality

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

**Step**

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use 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

### Step 3: Verifying LIFs and registering the serial number

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

**Steps**

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

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

2. Register the system serial number with NetApp Support.
   - 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. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto -giveback true`

### Step 4 (MetroCluster only): Switching back aggregates in a two-node MetroCluster configuration

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

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.

#### 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 & Replacements page for further information.

### Hot-swap a de-stage controller power module (DCPM) - AFF A700 and FAS9000

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.

#### Replacing 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.

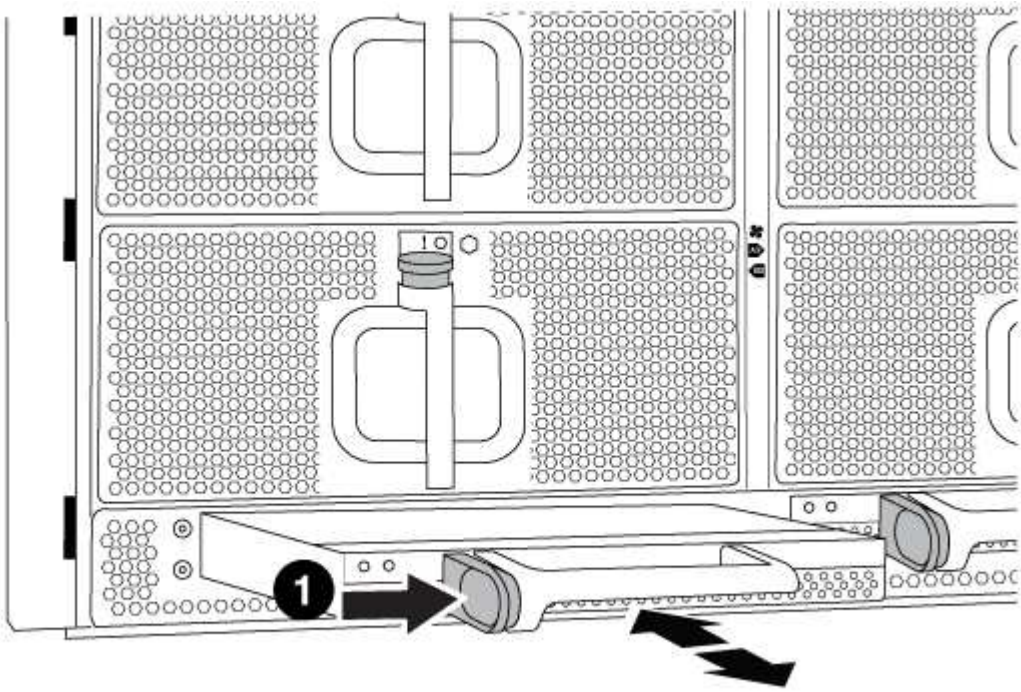
#### Steps

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.

#### 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

#### 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 & Replacements page for further information.

## Replace a DIMM - AFF A700 and FAS9000

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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: -
```

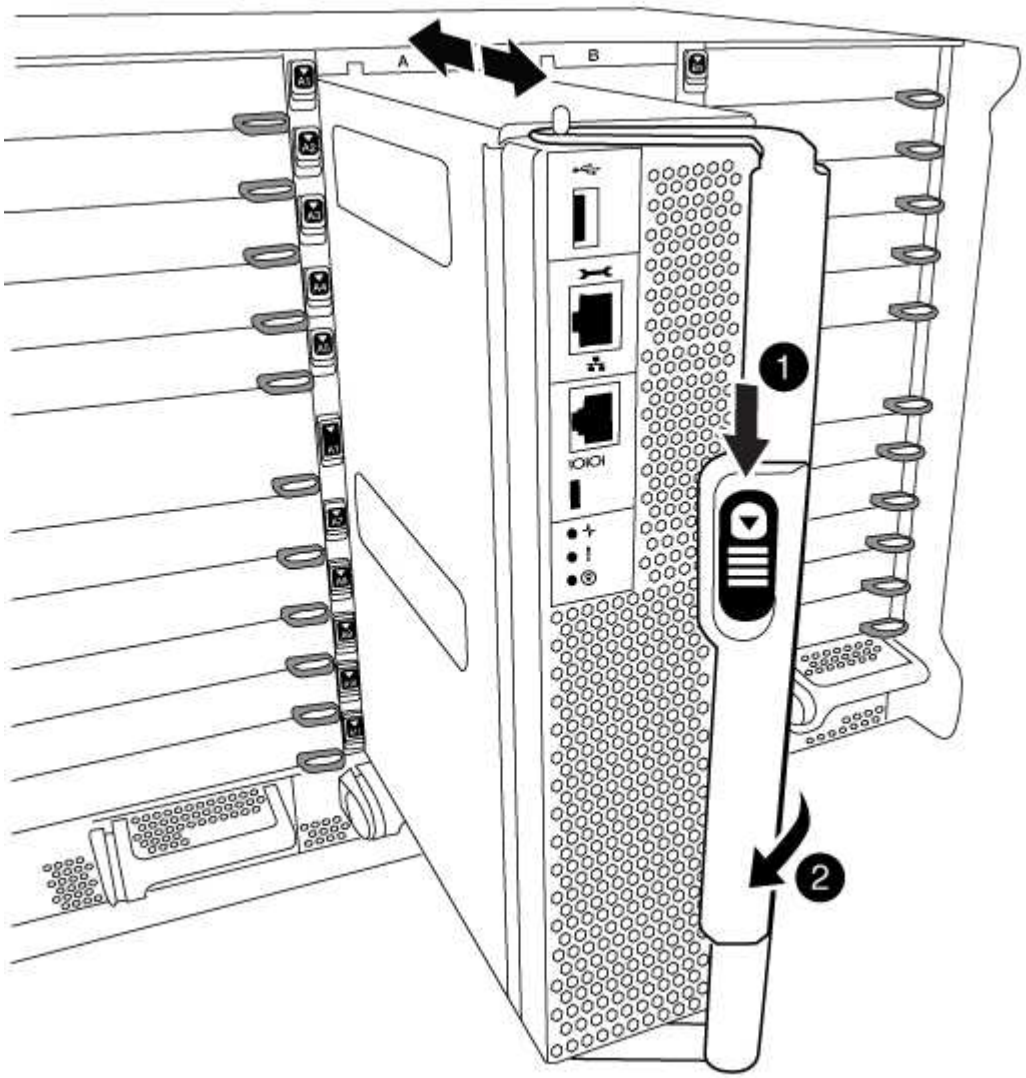
8. On the impaired controller module, disconnect the power supplies.

#### 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.



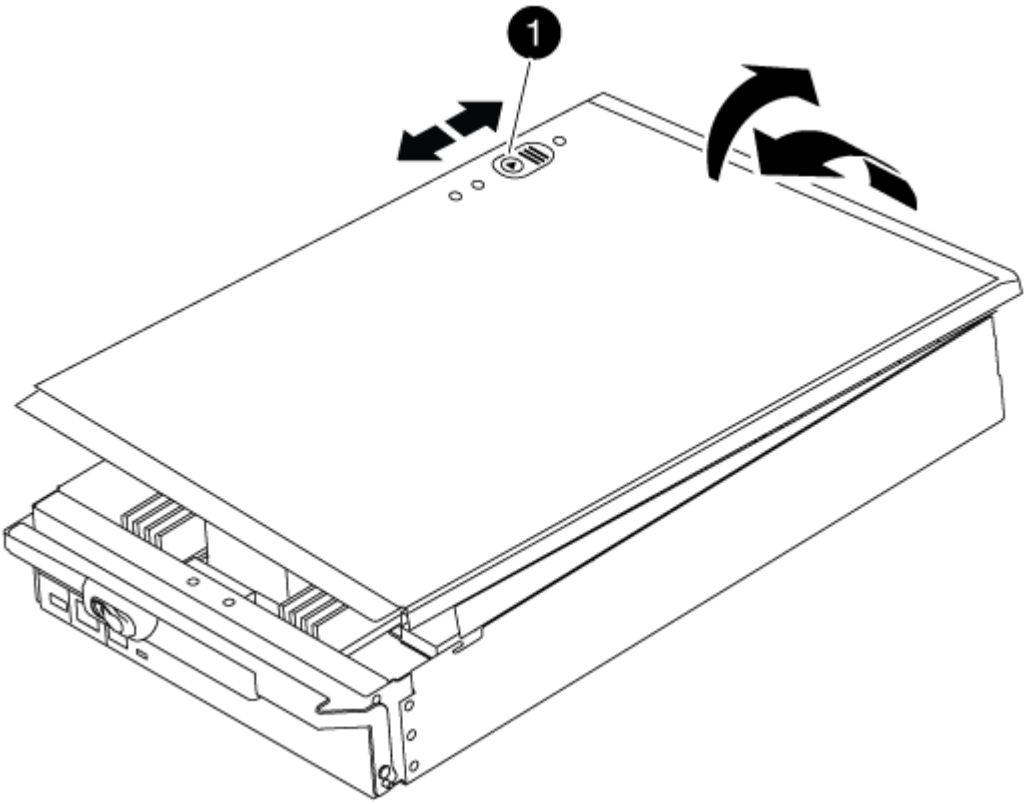

| | |
|---|---|
| 1 | Cam handle release button |

| | |
|---|---|
| ❷ | 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.




| | |
|---|---|
| ❶ | Controller module cover locking button |

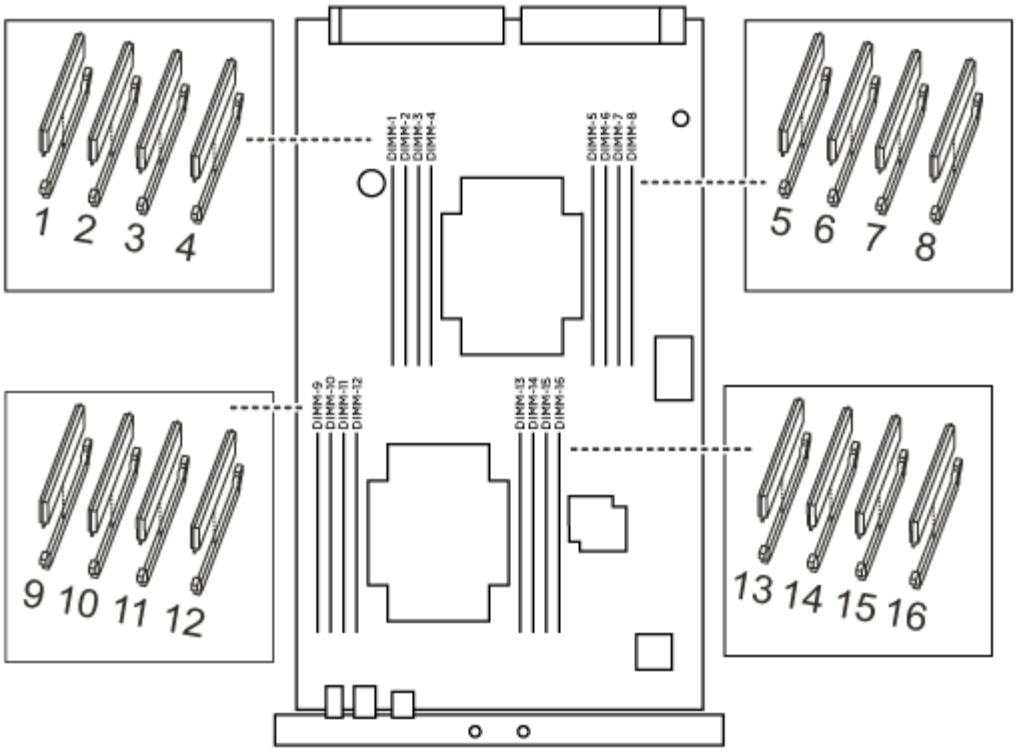
#### Step 3: Replace the DIMMs

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

**Steps**

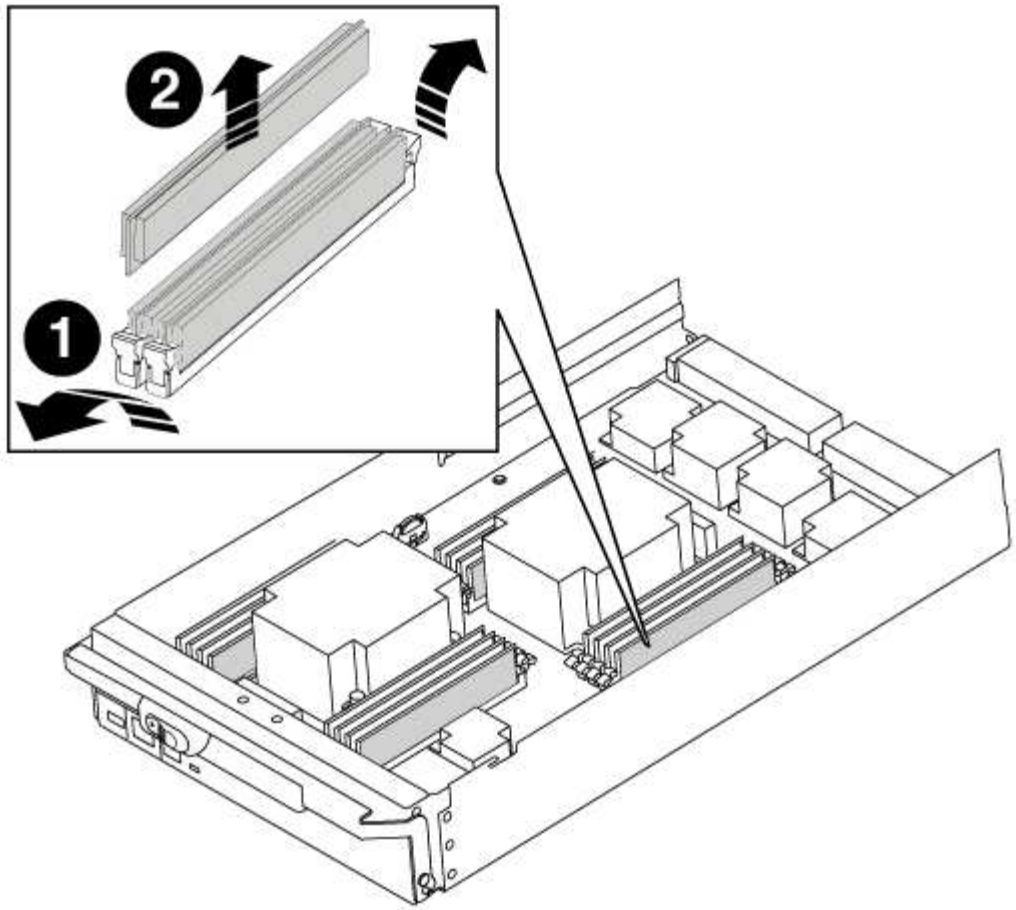
1. If you are not already grounded, properly ground yourself.
2. Locate the DIMMs on your controller module.

> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.




3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

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



| | |
|---|---|
| 1 | DIMM ejector tabs |
| 2 | DIMM |

4. 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.

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

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

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

6. 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.
7. 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. 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.

#### Step 5: Run system-level diagnostics

## After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

**Steps**

1. If the node to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.

b. After the node boots to Maintenance mode, halt the node: `halt`

After you issue the command, you should wait until the system stops at the LOADER prompt.

> During the boot process, you can safely respond `y` to prompts:

- A prompt warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy node remains down.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

| **If the system-level diagnostics tests…** | **Then…** |
|---|---|
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>*SLDIAG: No log messages are present.*<br>a. Exit Maintenance mode: `halt`<br>The node displays the LOADER prompt.<br>b. Boot the node from the LOADER prompt: `bye`<br>c. Return the node to normal operation. |
| An HA pair | Perform a give back: `storage failover giveback -ofnode` *`replacement_node_name`*<br>If you disabled automatic giveback, re-enable it with the storage failover modify command. |

| If the system-level diagnostics tests… | Then… |
| --- | --- |
| A two-node MetroCluster configuration | Proceed to the next step.<br><br>The MetroCluster switchback procedure is done in the next task in the replacement process. |
| A stand-alone configuration | Proceed to the next step.<br><br>No action is required.<br><br>You have completed system-level diagnostics. |
| Resulted in some test failures | Determine the cause of the problem:<br><br>a. Exit Maintenance mode: `halt`<br><br>After you issue the command, wait until the system stops at the LOADER prompt.<br><br>b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis:<br>◦ If you have two controller modules in the chassis, leave the power supplies turned on to provide power to the other controller module.<br>◦ If you have one controller module in the chassis, turn off the power supplies and unplug them from the power sources.<br>c. Verify that you have observed all the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu:<br>◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis.<br><br>The controller module boots up when fully seated.<br><br>◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on.<br>e. Select Boot to maintenance mode from the menu.<br>f. Exit Maintenance mode by entering the following command: `halt`<br><br>After you issue the command, wait until the system stops at the LOADER prompt.<br><br>g. Rerun the system-level diagnostic test. |

#### Step 6: Switch back aggregates in a two-node MetroCluster configuration

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

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 7: 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 & Replacements page for further information.

### Swap out a fan - AFF A700 and FAS9000

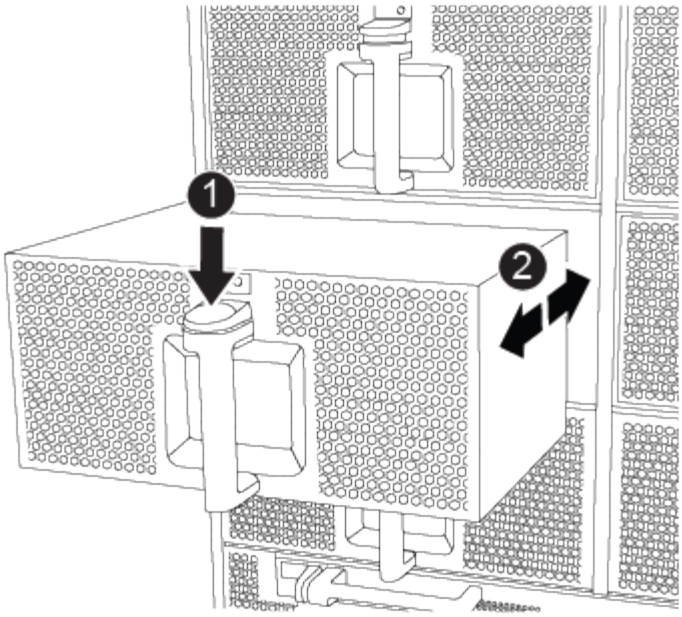
To swap out a fan module without interrupting service, you must perform a specific sequence of tasks.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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.

#### 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.

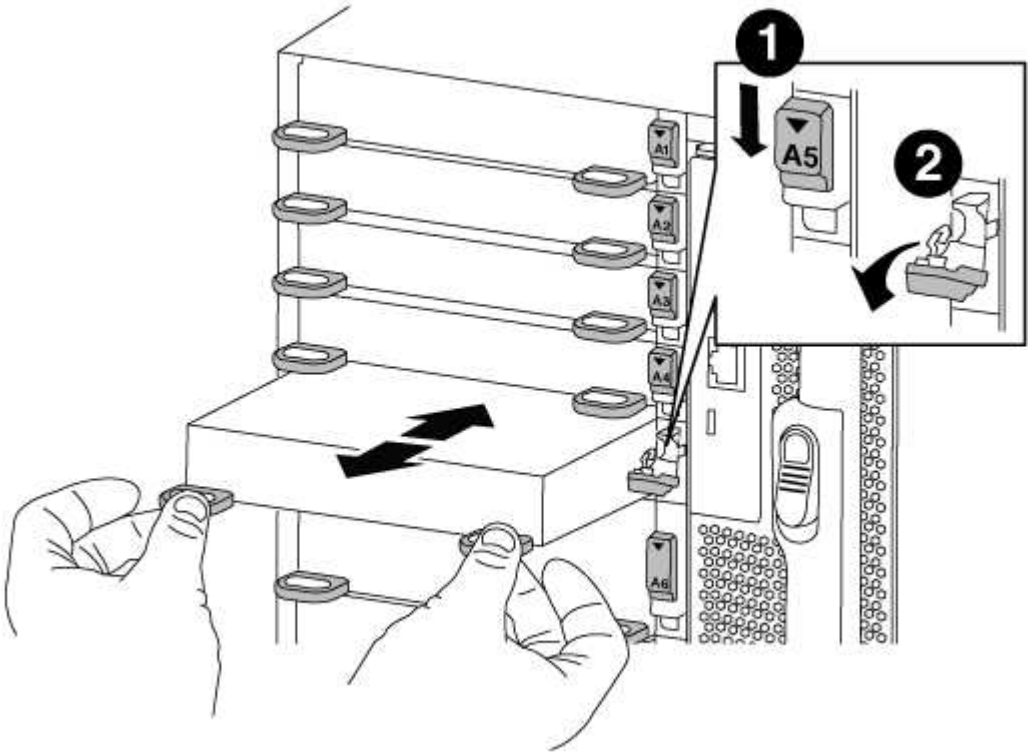
      The cam button moves away from the chassis.

   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.



| | |
|---|---|
| ❶ | Lettered and numbered I/O cam latch |
| ❷ | 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 PCIe module replacement

After you replace a PCIe module, you must reboot the controller module.

**Steps**

1. If the node is at the LOADER prompt, boot the node, responding `y` if you see a prompt warning of a system ID mismatch and asking to override the system ID: `bye`
2. 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.

3. Return the node to normal operation:

| If your system is in… | Issue this command from the partner's console… |
|---|---|
| An HA pair | `storage failover giveback -ofnode` *`impaired_node_name`* |
| A two-node MetroCluster configuration | Proceed to the next step.<br><br>The MetroCluster switchback procedure is done in the next task in the replacement process. |

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

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

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

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 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 & Replacements page for further information.

### Replace an LED USB module - AFF A700 and FAS9000

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 & Replacements page for further information.

### Replace the NVRAM module or NVRAM DIMMs - AFF A700 and FAS9000

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

#### Before you begin

- All disk shelves must be working properly.
- If your system is in an HA pair, the partner node must be able to take over the node associated with the NVRAM module that is being replaced.
- 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 are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Returning SEDs to unprotected mode" section of the *ONTAP 9 NetApp Encryption Power Guide*.

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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**

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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: -
```

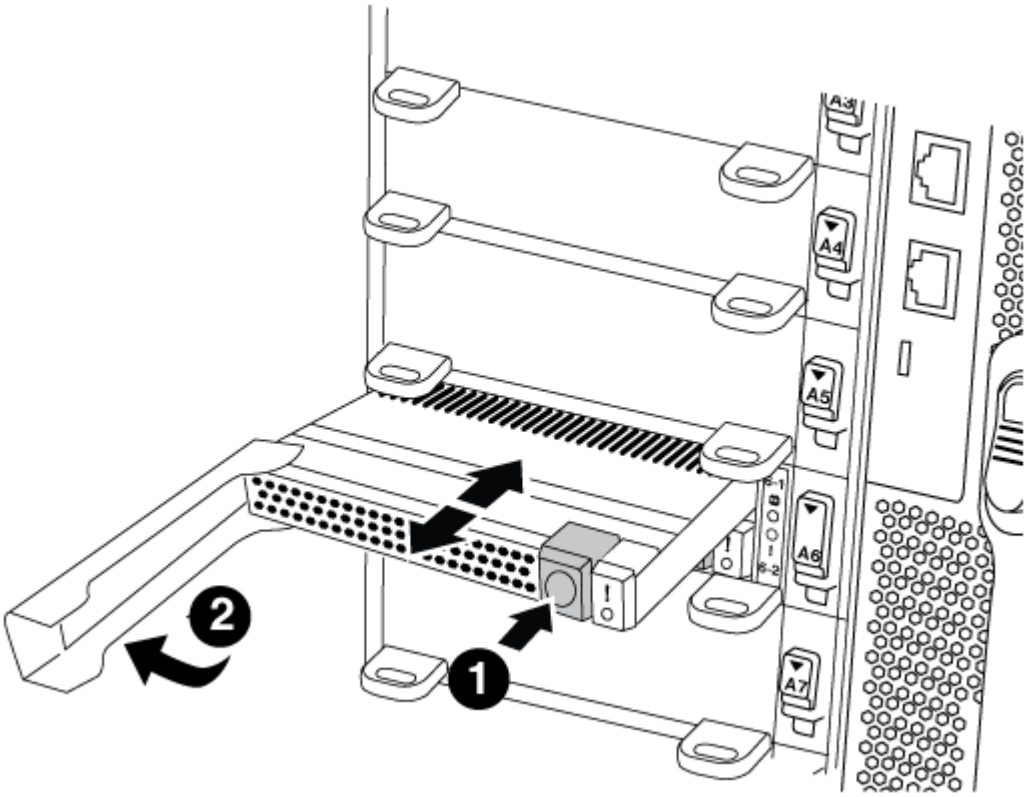
8. On the impaired controller module, disconnect the power supplies.

#### 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 FlashCache module from the old NVRAM module to the new NVRAM module:




| | |
|---|---|
| 1 | Orange release button (gray on empty FlashCache modules) |
| 2 | FlashCache cam handle |

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

> The release button on empty FlashCache modules is gray.

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

handle closed until it locks the module in place.

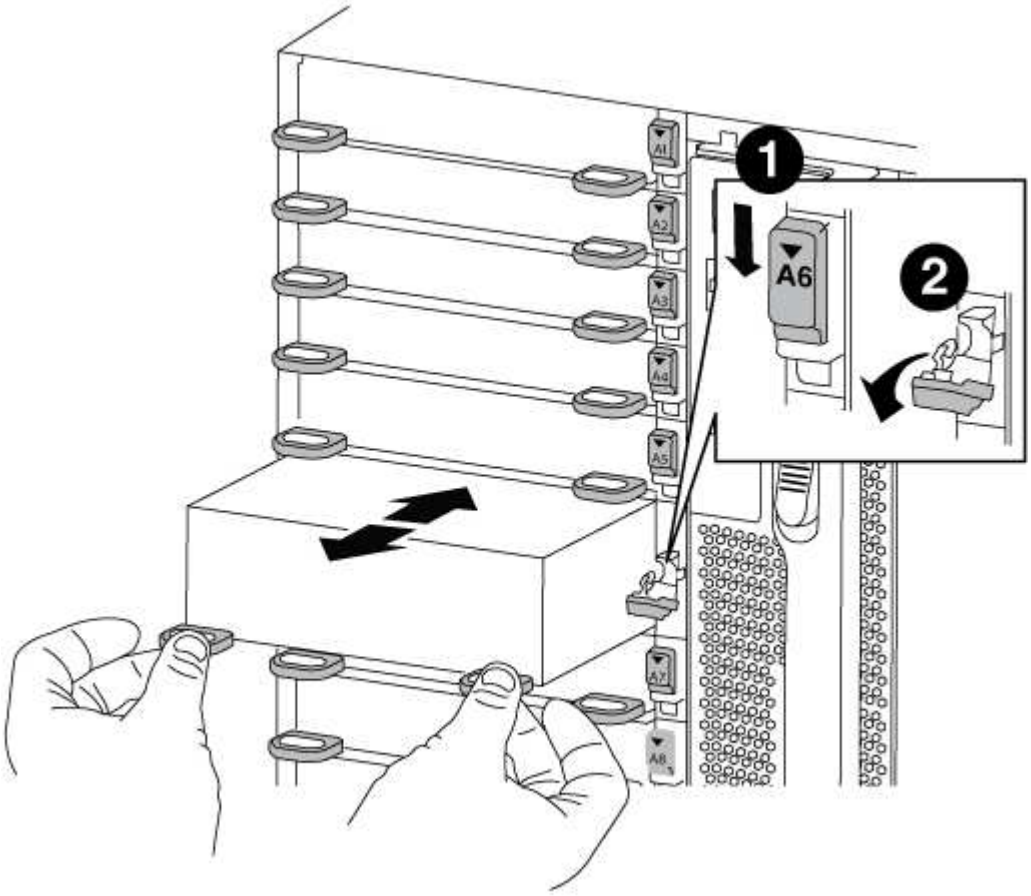
3. Remove the target NVRAM module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

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

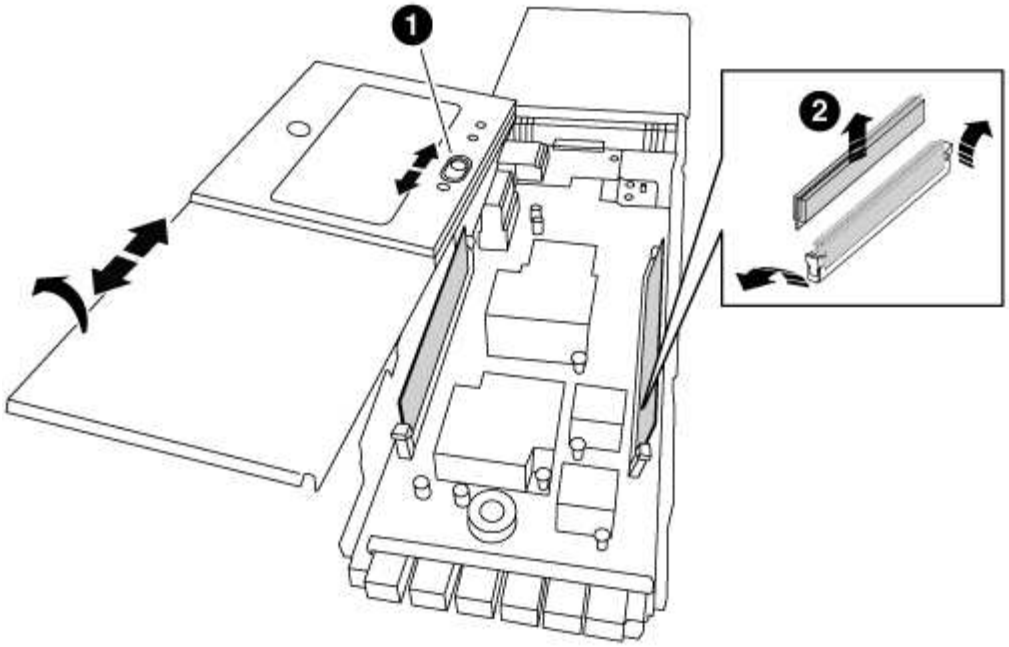
      The NVRAM module disengages from the chassis and moves out a few inches.

   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**

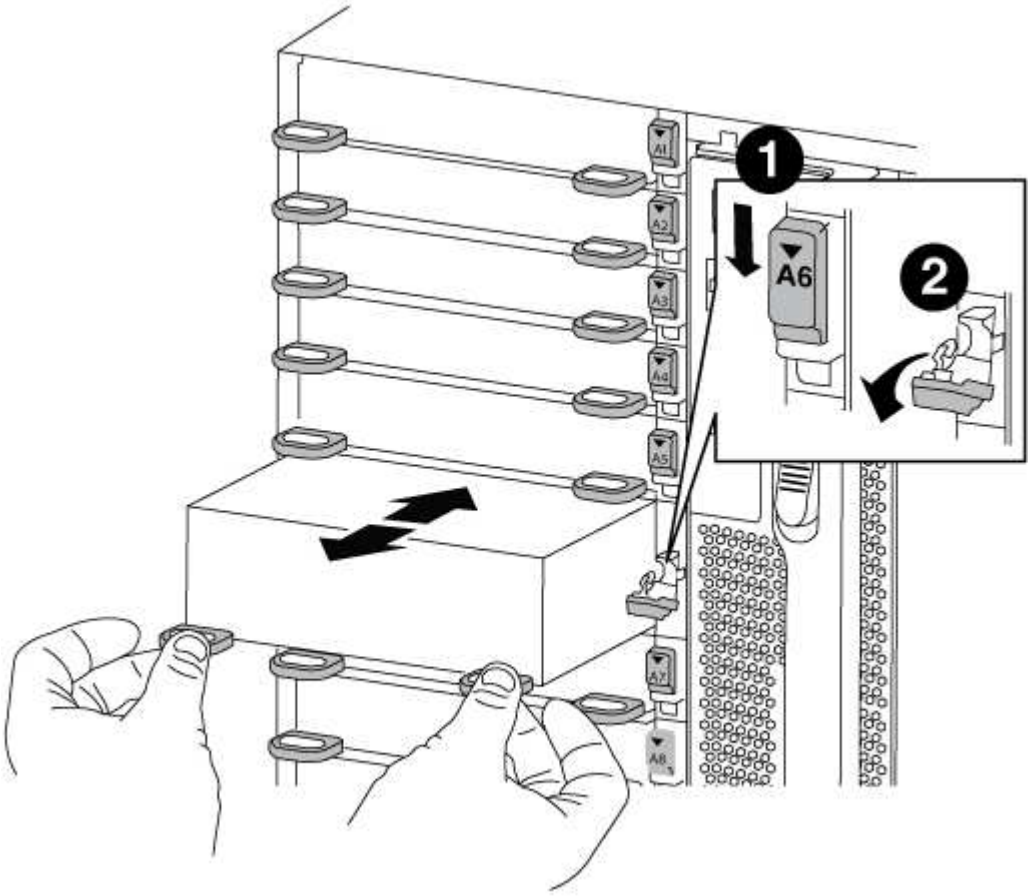
1. If you are not already grounded, properly ground yourself.
2. Remove the target NVRAM module from the chassis:
   a. Depress the lettered and numbered cam button.

      The cam button moves away from the chassis.

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

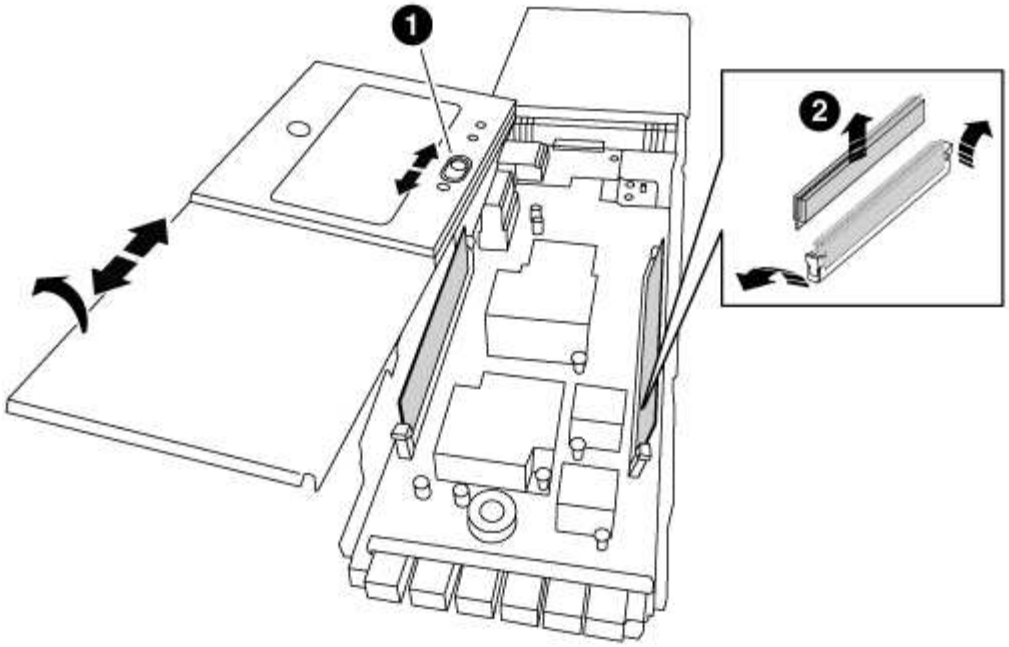
      The NVRAM module disengages from the chassis and moves out a few inches.

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.

   Each DIMM has an LED next to it that flashes when the DIMM has failed.

5. Install the replacement DIMM by aligning the DIMM with the socket and gently pushing the DIMM into the socket until the locking tabs lock in place.
6. Close the cover on the module.
7. Install the replacement NVRAM module into the chassis:
   a. Align the module with the edges of the chassis opening in slot 6.
   b. Gently slide the module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

#### 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.

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

**Steps**

1. If the replacement node is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the replacement node, boot the node, entering `y` if you are prompted to override the system ID due to a system ID mismatch.

   ```
   boot_ontap 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`
                                        Takeover
   Node              Partner            Possible     State Description
   ------------      ------------       --------
   -------------------------------------
   node1             node2              false        System ID changed
   on partner (Old:
                                                     151759755, New:
   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 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

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) or LUN ownership (for FlexArray systems), by using the system ID information obtained from the disk show command: `disk reassign -s old system ID`

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

   You can respond `Y` when prompted to continue.

5. Verify that the disks (or FlexArray LUNs) were assigned correctly: `disk show -a`

   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   system-1  (118065481) Pool0  J8Y0TDZC       system-1
(118065481)
disk_name   system-1  (118065481) Pool0  J8Y09DXC       system-1
(118065481)
.
.
.
```

6. From the healthy node, verify that any coredumps are saved:
   a. Change to the advanced privilege level: `set -privilege advanced`

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

   b. Verify that the coredumps are saved: `system node run -node` *`local-node-name`* `partner savecore`

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

   c. Return to the admin privilege level: `set -privilege admin`
7. If the *replacement* node is in Maintenance mode (showing the *> prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
8. Boot the *replacement* node: `boot_ontap`
9. After the *replacement* node has fully booted, perform a switchback: `metrocluster switchback`
10. Verify the MetroCluster configuration: `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: Restore Storage and Volume Encryption functionality

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

**Step**

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use 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

#### Step 7: 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 & Replacements page for further information.

### Swap out a power supply - AFF A700 and FAS9000

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.
- 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.

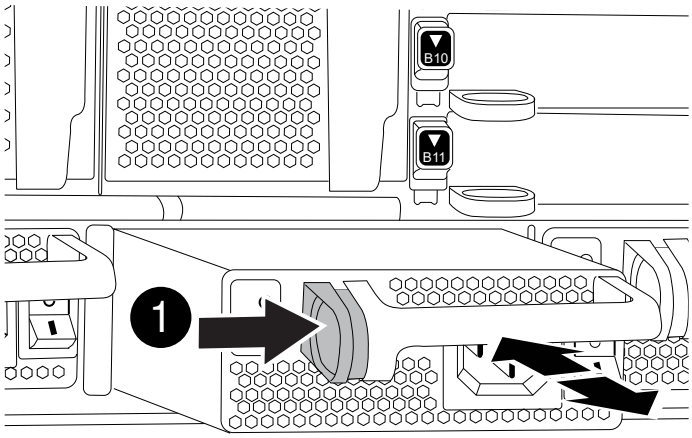
- The number of power supplies in the system depends on the model.
- Power supplies are auto-ranging.

> 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 & Replacements page for further information.

**Replace the real-time clock battery**

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.

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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

- If you are using NetApp Storage Encryption, you must have reset the MSID using the instructions in the "Return a FIPS drive or SED to unprotected mode" section of NetApp Encryption overview with the CLI.
- 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: `metrocluster switchover` |
| Has not automatically switched over, you attempted switchover with the `metrocluster switchover` 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: -
```

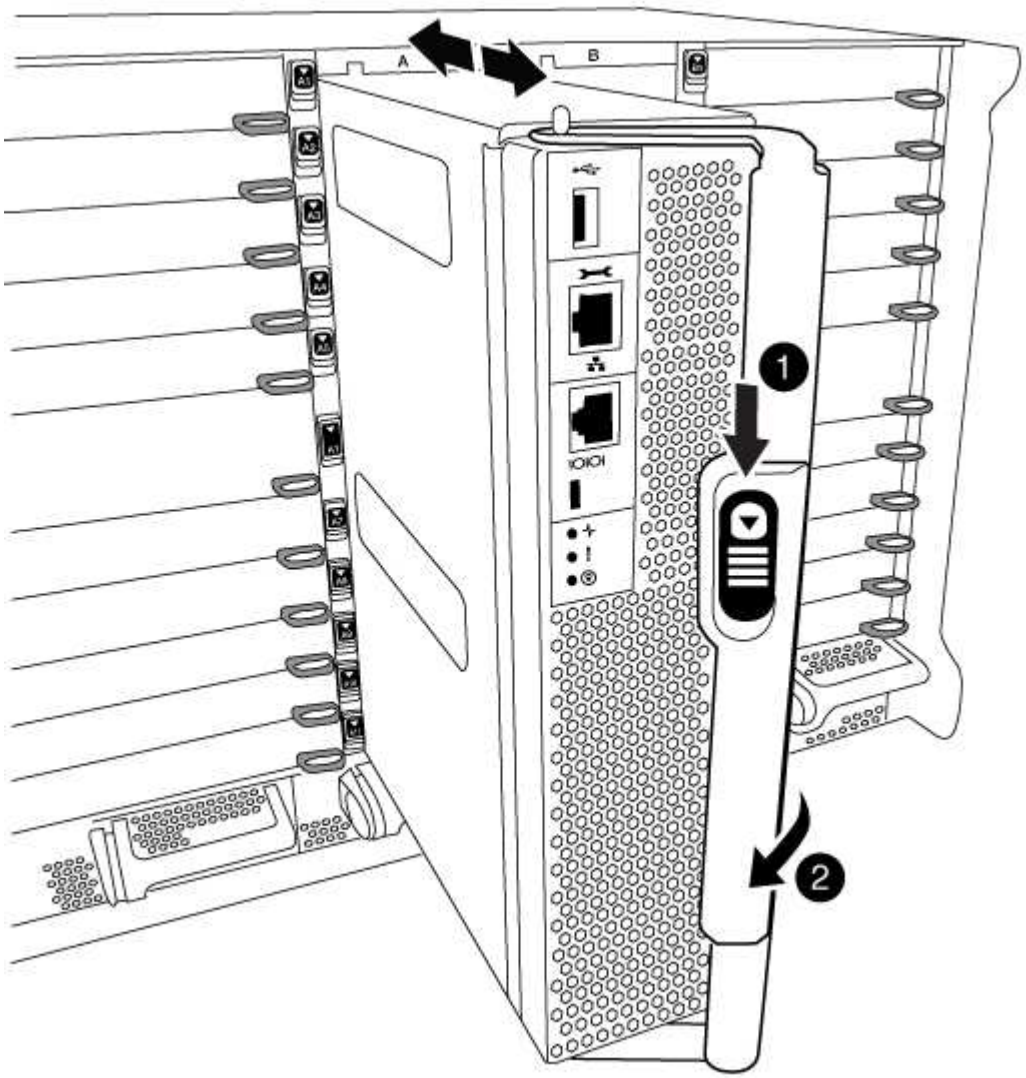
8. On the impaired controller module, disconnect the power supplies.

#### 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.



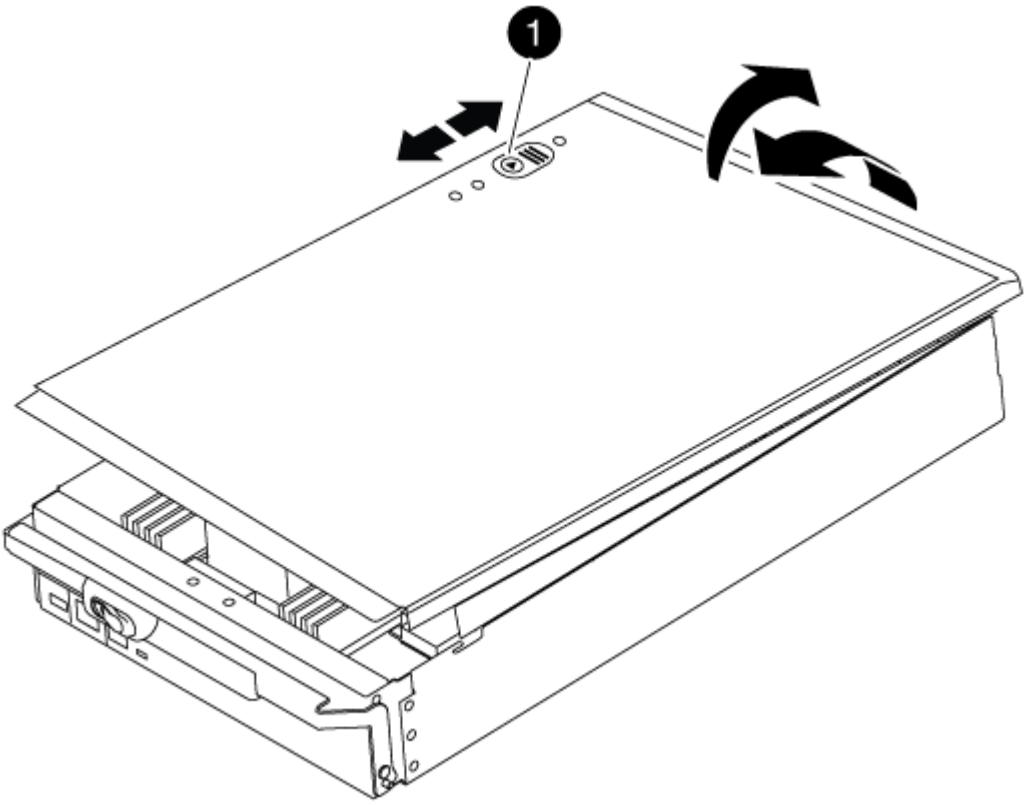

| | |
|---|---|
| 1 | Cam handle release button |

| | |
|---|---|
| ❷ | 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.



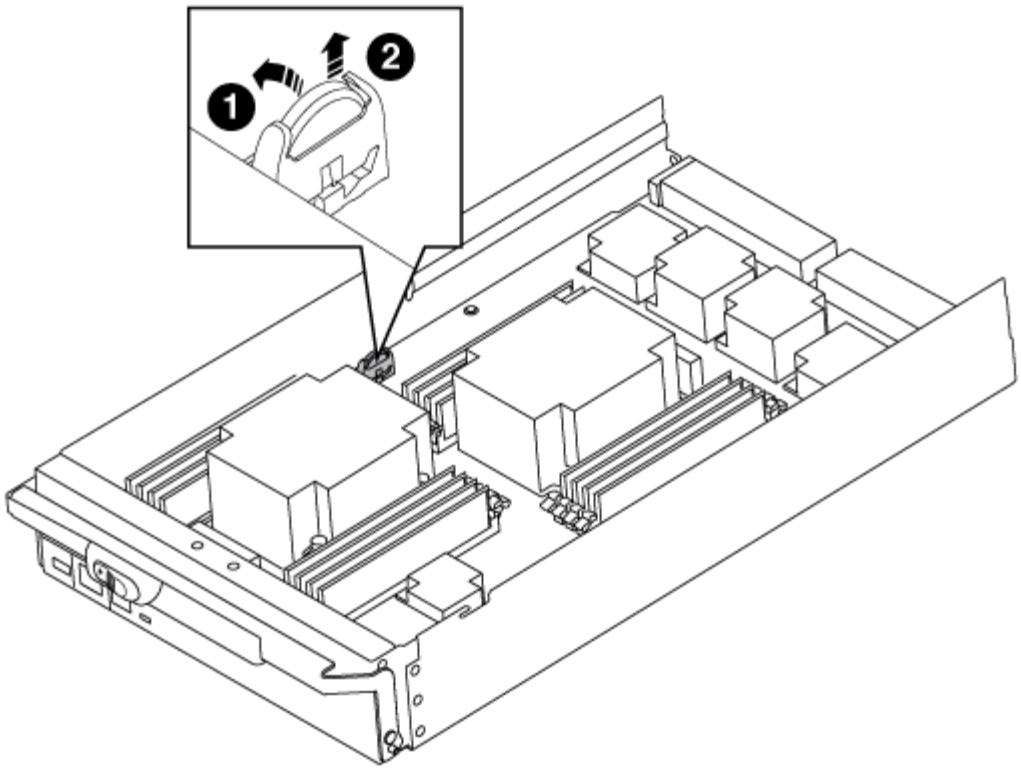

| | |
|---|---|
| ❶ | Controller module cover locking button |

#### 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

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

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 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 & Replacements page for further information.

### X91148A module

#### Overview of adding an X91148A module - AFF A9000

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 an AFF A700 with open slots - AFF A700 and FAS9000

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 Hardware Universe.

  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 Hardware Universe for other slots that can be used by the X91148A module for networking.

  NetApp Hardware Universe

- 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 in a system with open slots

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: `boot_ontap`
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 in a system with open slots

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: `boot_ontap`
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 - NS224 shelves.

#### Add an X91148A storage module in a system with no open slots - AFF A700 and FAS9000

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 Hardware Universe for other slots that can be used by the X91148A module for networking.

  NetApp Hardware Universe

- 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 in a system with no open slots

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**

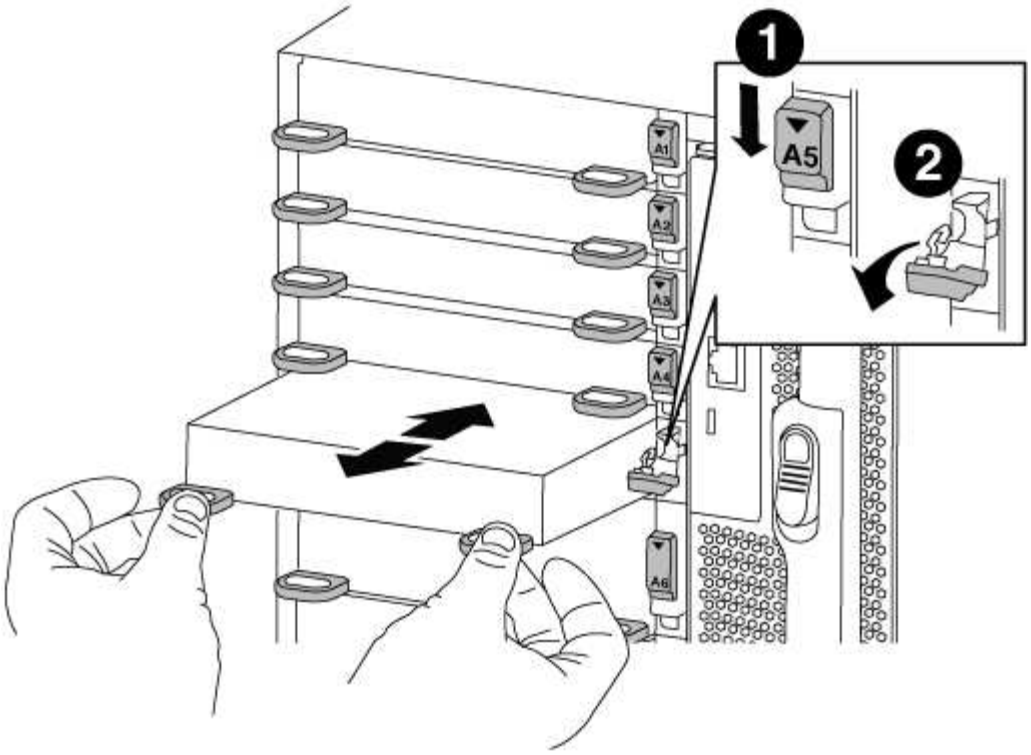
1. If you are adding an X91148A module into a slot that contains a NIC module with the same number of ports as the X91148A module, the LIFs will automatically migrate when its controller module is shut down. If the NIC module being replaced has more ports than the X91148A module, you must permanently 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.




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

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: `boot_ontap`
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 in a system with no open slots

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**

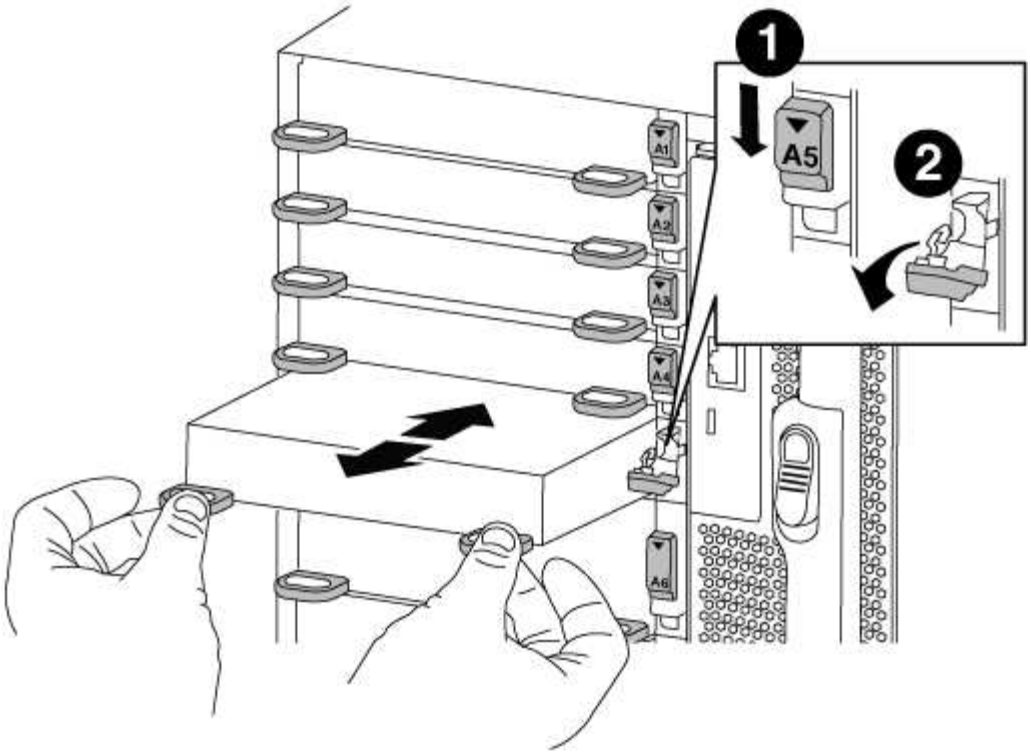
1. If you are adding an X91148A module as a storage module in slots 3 and/or 7 into a slot that has an existing NIC module in it, use System Manager to permanently migrate the LIFs to different home ports, as described in Migrating a LIF.
2. Shut down controller A:
   a. Disable automatic giveback: `storage 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.




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

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: `boot_ontap`
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-adding an NS224 drive shelf.

# FAS9500 systems

## Install and setup

### Start here: Choose your installation and setup experience

You can choose from different content formats to guide you through installing and setting up your new storage system.

- Quick steps

  A printable PDF of step-by-step instructions with live links to additional content.

- Video steps

  Video step-by-step instructions.

- Detailed steps

  Online step-by-step instructions with live links to additional content.

### Quick steps - FAS9500

This topic gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use this content if you are familiar with installing NetApp systems.

Access the *Installation and Setup Instructions* PDF poster:

FAS9500 Installation and Setup Instructions

### Video steps - FAS9500

There are two videos - one showing how to rack and cable your system and one showing an example of using the System Manager Guided Setup to perform initial system configuration.

#### Video one of two: Hardware installation and cabling

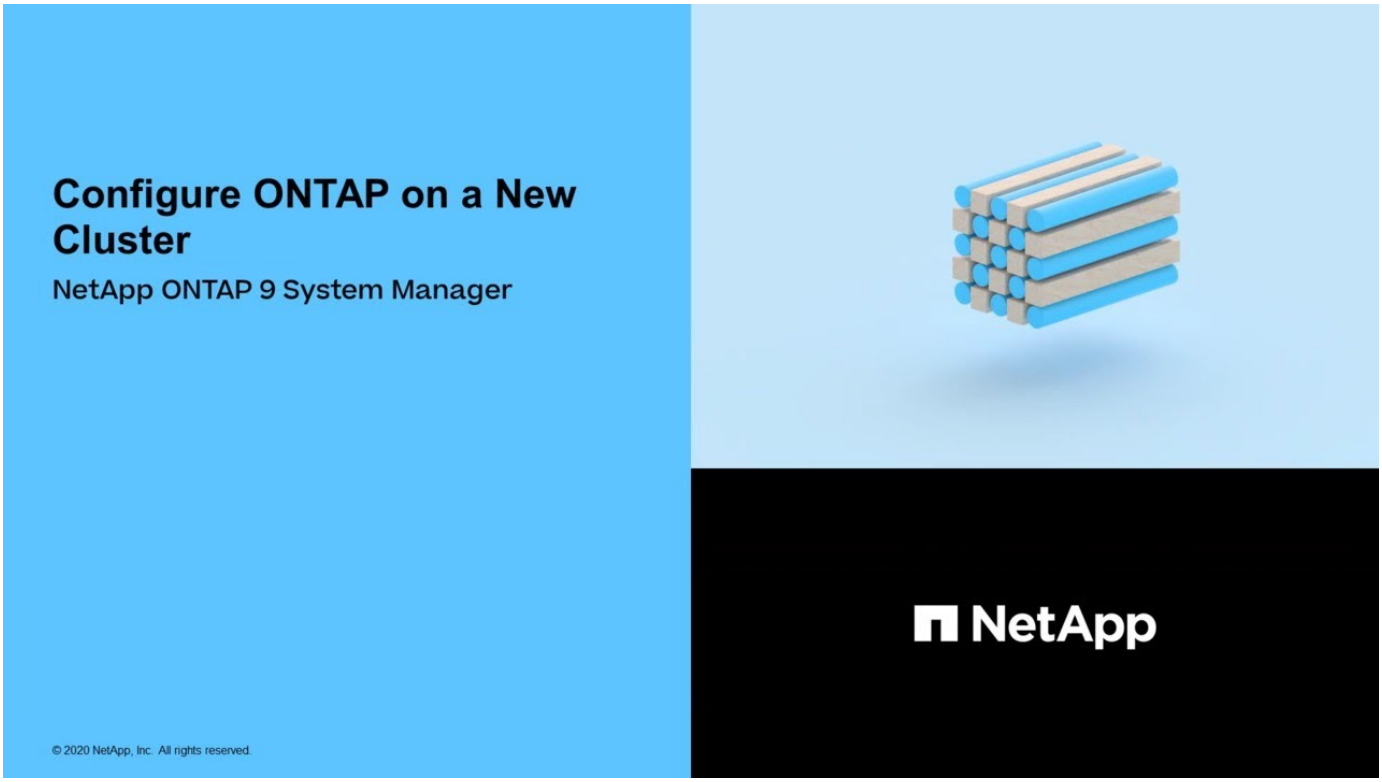
The following video shows how to install and cable your new system.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=ab45062
1-9e1c-44a7-befa-ae7c01708d9e" width="711"> </iframe></div>
```

Animation - Animated Installation and setup instructions - FAS9500

#### Video two of two: Performing end-to-end software configuration

The following video shows end-to-end software configuration for systems running ONTAP 9.6 and later.




### Detailed steps - FAS9500

This article gives detailed step-by-step instructions for installing a typical NetApp system. Use this article if you want more detailed installation instructions.

#### Step 1: Prepare for installation

To install your system, you need to create an account on the NetApp Support Site, register your system, and get license keys. You also need to inventory the appropriate number and type of cables for your system and collect specific network information.

You need to have access to the NetApp Hardware Universe for information about site requirements as well as additional information on your configured system.

**What you need**

You might also want to have access to the ONTAP 9 Release Notes for your version of ONTAP for more information about this system.

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser

**Steps**

1. Unpack the contents of all boxes.
2. Record the system serial number from the controllers.

3. Inventory and make a note of the number and types of cables you received.

   The following table identifies the types of cables you might receive. If you receive a cable not listed in the table, see the Hardware Universe to locate the cable and identify its use.

   NetApp Hardware Universe

| Type of cable… | Part number and length | Connector type | For… |
|---|---|---|---|
| 25 GbE data Cable | X66240A-05 (112-00639), 0.5m<br>X66240A-2 (112-00598), 2m<br>X66240A-5 (112-00600), 5m | | Network cable |
| 32 Gb FC (SFP+ Op) | X66250-2 (112-00342), 2m<br>X66250-5 (112-00344), 5m<br>X66250-15 (112-00346), 15m | | FC optical network cable |
| 40 GbE network cable | X66100-1 (112-00542), 1m<br>X66100-3 (112-00543), 3m<br>X66100-5 (112-00544), 5m | | Ethernet data, cluster network |
| 100 GbE cable | X66211B-1 (112-00573), 1m<br>X66211B-2 (112-00574), 2m<br>X66211B-5 (112-00576), 5m | | Network,<br>Ethernet data,<br>cluster network |
| Optical cables | X66031A (112-00436), 1m<br>X66032A (112-00437), 2m<br>X66033A (112-00438), 3m | | FC optical network |
| Cat 6, RJ-45 (order dependent) | Part numbers X6585-R6 (112-00291), 3m<br>X6562-R6 (112-00196), 5m | | Management network and Ethernet data |

| Type of cable… | Part number and length | Connector type | For… |
|---|---|---|---|
| Storage | X66031A (112-00436), 1m<br>X66032A (112-00437), 2m<br>X66033A (112-00438), 3m | | Storage |
| Micro-USB console cable | Not applicable | | Console connection during software setup on non-Windows or Mac laptop/console |
| Power cables | Not applicable | | Powering up the system |

4. Review the ONTAP Configuration Guide and collect the required information listed in that guide.

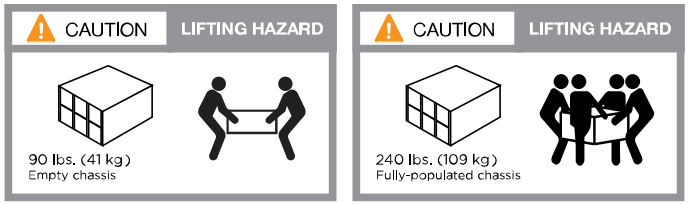
#### Step 2: Install the hardware

You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

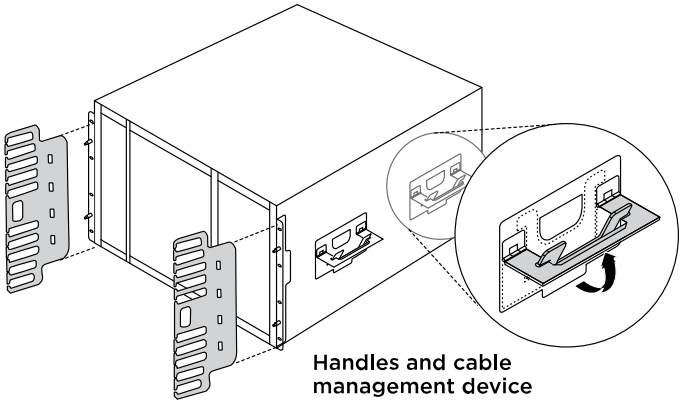
1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.

   You need to be aware of the safety concerns associated with the weight of the system.

   The label on the left indicates an empty chassis, while the label on the right indicates a fully-populated system.




3. Attach cable management devices (as shown).




4. Place the bezel on the front of the system.

#### Step 3: Cable controllers to your network

You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

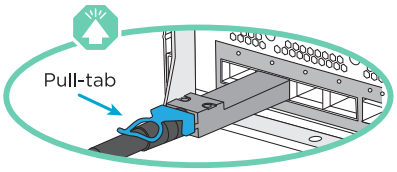
**Option 1: Two-node switchless cluster**

Management network, data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled on both controllers.

**Before you begin**

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all networking module ports.

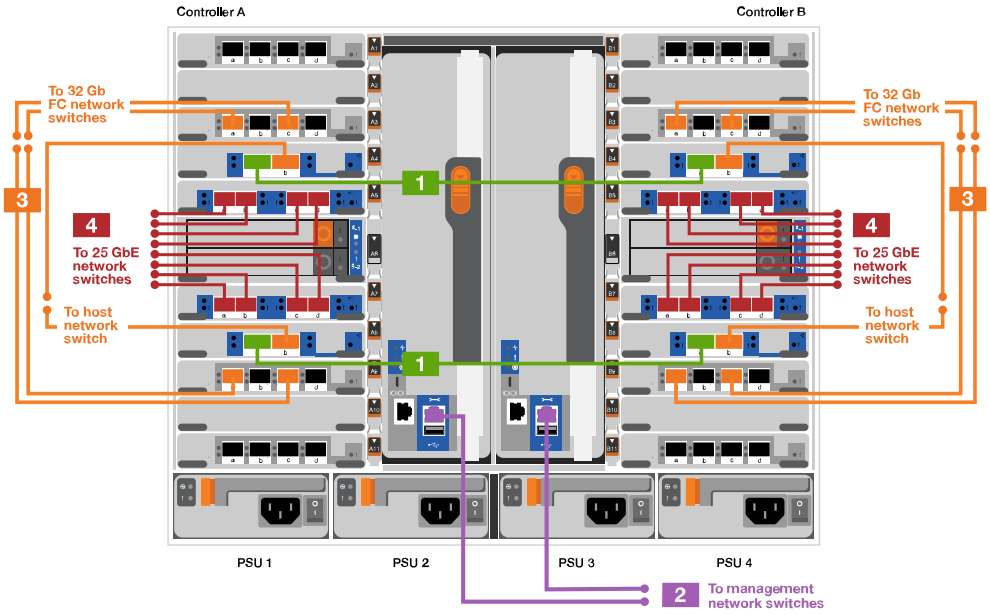



As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it over and try again.

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=d
a08295f-ba8c-4de7-88c3-ae7c0170408d" width="711"> </iframe></div>
```

Animation - Two-node switchless cluster cabling



| Step | Perform on each controller |
|---|---|
| 1 | Cable cluster interconnect ports:<br>• Slot A4 and B4 (e4a)<br>• Slot A8 and B8 (e8a)<br> |
| 2 | Cable controller management (wrench) ports.<br> |
| 3 | Cable 32 Gb FC network switches:<br><br>Ports in slot A3 and B3 (e3a and e3c) and slot A9 and B9 (e9a and e9c) to the 32 Gb FC network switches.<br> <br><br>40GbE host network switches:<br><br>Cable host-side b ports in slot A4 and B4 (e4b) and slot A8 and B8 (e8b) to the host switch.<br> |
| 4 | Cable 25 GbE connections:<br><br>Cable ports in slot A5 and B5 (5a, 5b, 5c, and 5d) and slot A7 and B7 (7a, 7b, 7c, and 7d) to the 25 GbE network switches.<br> |

2. Connect the power cables to the PSUs and connect them to different power sources (not shown).
3. Strap the cables to the cable management arms (not shown).
4. To cable your storage, see Step 4: Cable controllers to drive shelves.

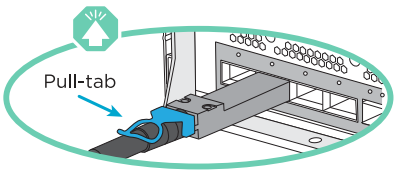
**Option 2: Switched cluster**

Management network, data network, and management ports on the controllers are connected to switches. The cluster interconnect and HA ports are cabled on to the cluster/HA switch.

**Before you begin**

You must have contacted your network administrator for information about connecting the system to the switches.

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all networking module ports.

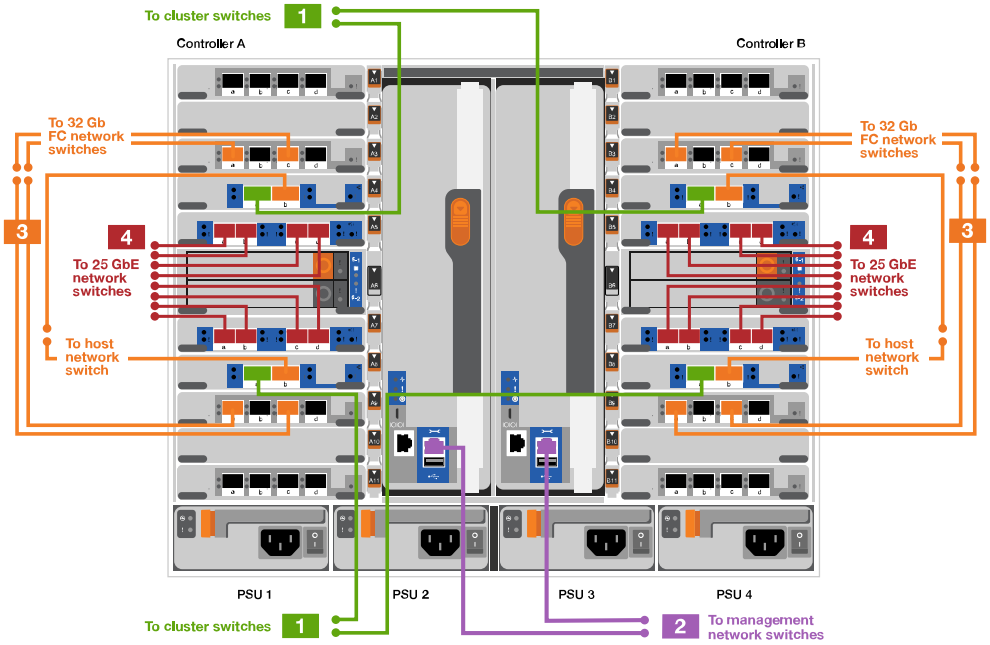



As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it over and try again.

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=3
ad3f118-8339-4683-865f-ae7c0170400c" width="711"> </iframe></div>
```

Animation - Switched cluster cabling



| Step | Perform on each controller |
|---|---|
| 1 | Cable cluster interconnect a ports:<br><br>• Slot A4 and B4 (e4a) to the cluster network switch.<br>• Slot A8 and B8 (e8a) to the cluster network switch.<br><br> |
| 2 | Cable controller management (wrench) ports.<br><br> |
| 3 | Cable 32 Gb FC network switches:<br><br>Ports in slot A3 and B3 (e3a and e3c) and slot A9 and B9 (e9a and e9c) to the 32 Gb FC network switches.<br><br> <br><br>40GbE host network switches:<br><br>Cable host-side b ports in slot A4 and B4 (e4b) and slot A8 and B8 (e8b) to the host switch.<br><br> |
| 4 | Cable 25 GbE connecions:<br><br>Cable ports in slot A5 and B5 (5a, 5b, 5c, and 5d) and slot A7 and B7 (7a, 7b, 7c, and 7d) to the 25 GbE network switches.<br><br> |

2. Connect the power cables to the PSUs and connect them to different power sources (not shown).
3. Strap the cables to the cable management arms (not shown).
4. To cable your storage, see Step 4: Cable controllers to drive shelves.

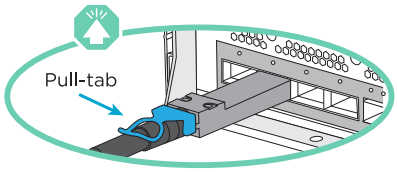
#### Step 4: Cable controllers to drive shelves

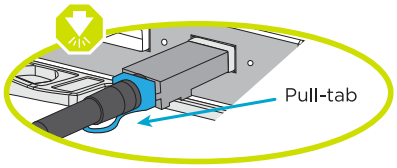
You must cable the shelf-to-shelf connections, and then cable both controllers to the DS212C or DS224C drive shelves.

For more SAS cabling information and worksheets, see SAS cabling rules, worksheets, and examples overview - shelves with IOM12 modules

**Before you begin**

- Complete the SAS cabling worksheet for your system. See SAS cabling rules, worksheets, and examples overview - shelves with IOM12 modules.
- Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the storage modules are up, while the pull tabs on the shelves are down.



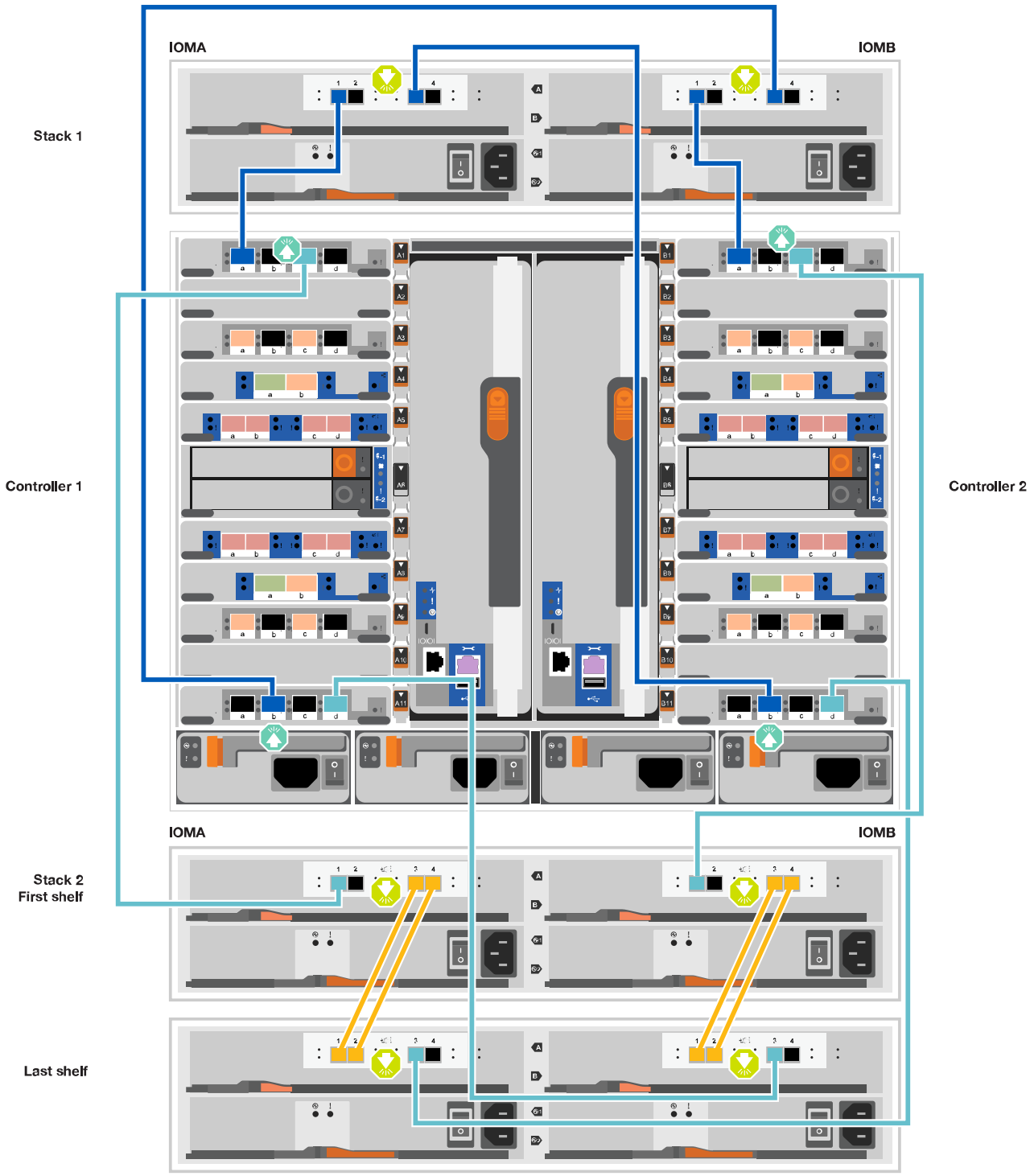




As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it over and try again.

1. Use the following animation or drawings to cable your controllers to three (1 stack of one drive shelf and one stack of two drive shelves) DS224C drive shelves.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=c958a
ae6-9d08-4d3d-a213-ae7c017040cd" width="711"> </iframe></div>
```

Animation - Cabling your drive shelves




| Step | Perform on each controller |
|---|---|
| 1 | Connect drive shelf stack one to the controllers, using the graphic for reference.<br> <br>mini-SAS cable |

| Step | Perform on each controller |
| --- | --- |
| 2 | Connect drive shelf stack two to the controllers, using the graphic for reference.<br> <br>mini-SAS cable |

2. To complete setting up your system, see Step 5: Complete system setup and configuration.

#### Step 5: Complete system setup and configuration

You can complete the system setup and configuration using cluster discovery with only a connection to the switch and laptop, or by connecting directly to a controller in the system and then connecting to the management switch.

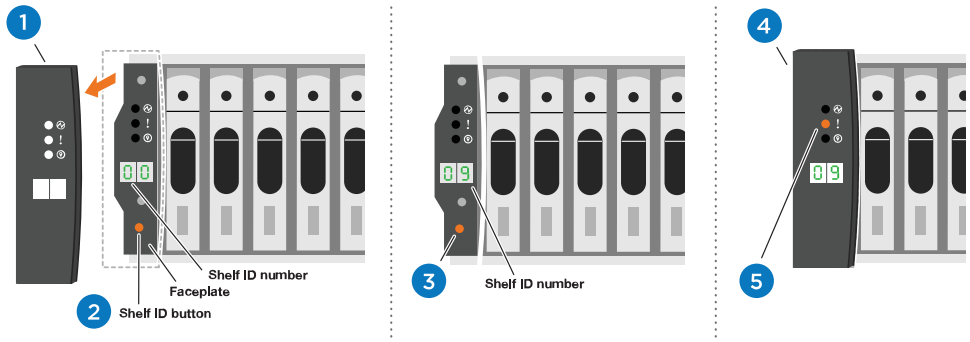
**Option 1: If network discovery is enabled**

If you have network discovery enabled on your laptop, you can complete system setup and configuration using automatic cluster discovery.

1. Use the following animation or drawing to set one or more drive shelf IDs:

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=9
5a29da1-faa3-4ceb-8a0b-ac7600675aa6" width="711"> </iframe></div>
```

Animation - Setting your shelf ID's

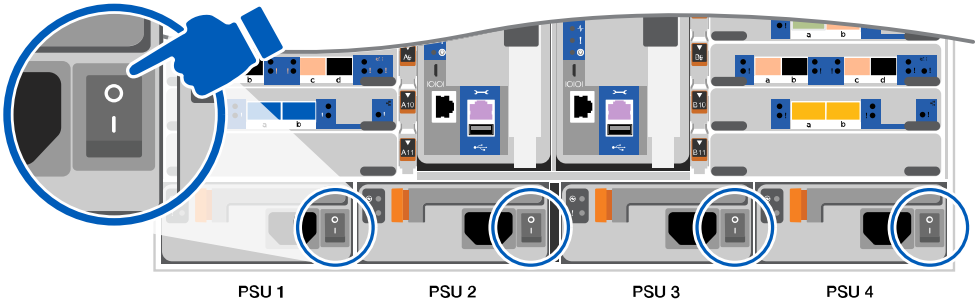



| | |
|---|---|
| 1 | Remove the end cap. |
| 2 | Press and hold shelf ID button until first digit blinks, then push to advance to 0-9.<br>ⓘ The first digit continues to blink |
| 3 | Press and hold shelf ID button until second digit blinks, then push to advance to 0-9.<br>ⓘ The first digit stops blinking, and the second digit continues to blink. |
| 4 | Replace the end cap. |
| 5 | Wait 10 seconds for the Amber LED (!) to appear, then power-cycle the drive shelf to set shelf ID. |

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Turn on the power switches to both nodes.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=a
905e56e-c995-4704-9673-adfa0005a891" width="711"> </iframe></div>
```

Animation - Turn on the power to the controllers




Initial booting may take up to eight minutes.

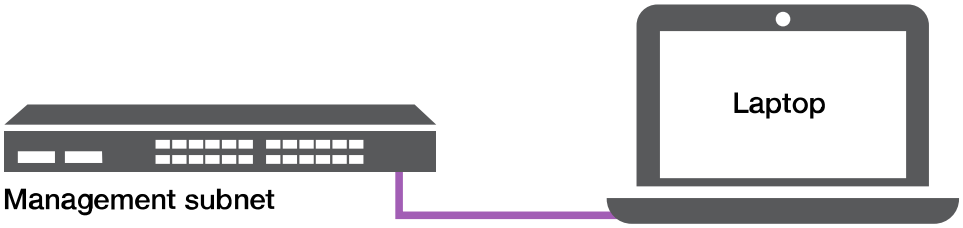
4. Make sure that your laptop has network discovery enabled.

   See your laptop's online help for more information.

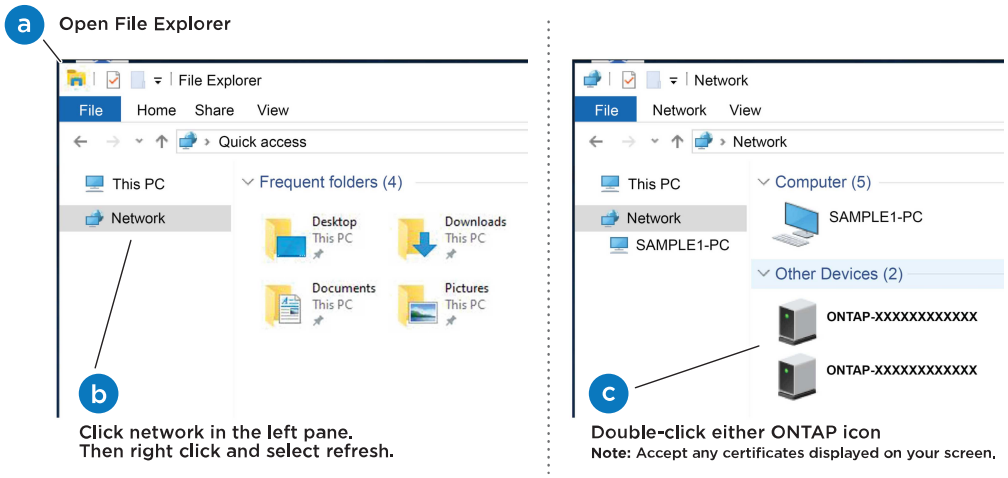
5. Use the following animation to connect your laptop to the Management switch.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=d
61f983e-f911-4b76-8b3a-ab1b0066909b" width="711"> </iframe></div>
```

Animation - Connecting your laptop to the Management switch




6. Select an ONTAP icon listed to discover:




a. Open File Explorer.
b. Click network in the left pane.
c. Right click and select refresh.
d. Double-click either ONTAP icon and accept any certificates displayed on your screen.

> XXXXX is the system serial number for the target node.

System Manager opens.

7. Use System Manager guided setup to configure your system using the data you collected in the ONTAP Configuration Guide.
8. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

   b. Register your system.

      NetApp Product Registration

   c. Download Active IQ Config Advisor.

      NetApp Downloads: Config Advisor
9. Verify the health of your system by running Config Advisor.
10. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

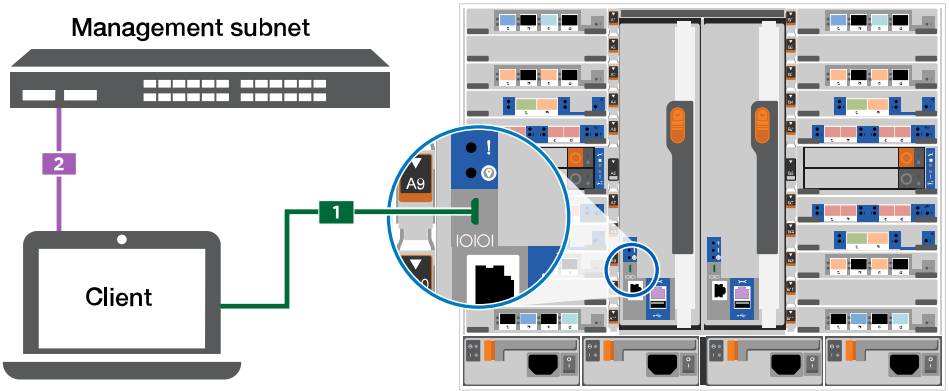
**Option 2: If network discovery is not enabled**

If you are not using a Windows or Mac-based laptop or console or if auto discovery is not enabled, you must complete the configuration and setup using this task.

1. Cable and configure your laptop or console:
   a. Set the console port on the laptop or console to 115,200 baud with N-8-1.

See your laptop or console's online help for how to configure the console port.

b. Connect the console cable to the laptop or console using the console cable that came with your system, and then connect the laptop to the switch on the management subnet.

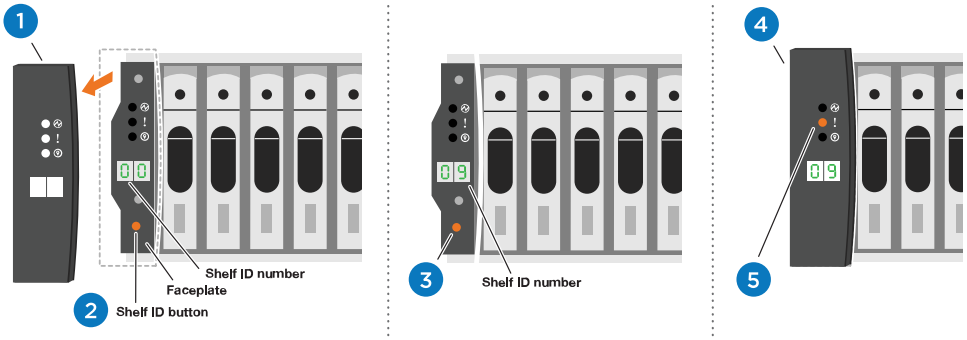



c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.

2. Use the following animation to set one or more drive shelf IDs:

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=9
5a29da1-faa3-4ceb-8a0b-ac7600675aa6" width="711"> </iframe></div>
```

Animation - Setting your shelf ID's



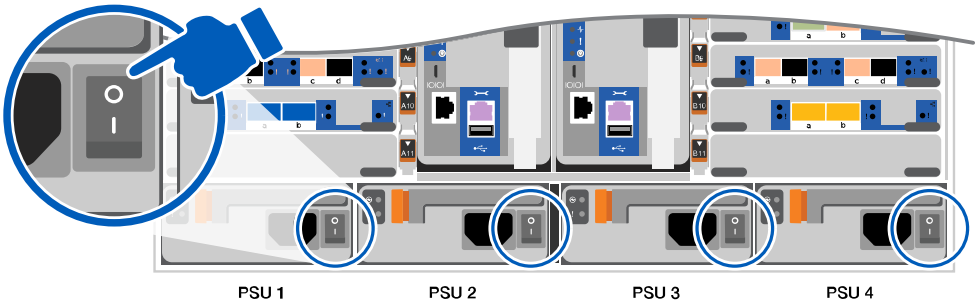

| | |
|---|---|
| 1 | Remove the end cap. |
| 2 | Press and hold shelf ID button until first digit blinks, then push to advance to 0-9.<br>The first digit continues to blink |

| | |
|---|---|
| ❸ | Press and hold shelf ID button until second digit blinks, then push to advance to 0-9.<br>ⓘ The first digit stops blinking, and the second digit continues to blink. |
| ❹ | Replace the end cap. |
| ❺ | Wait 10 seconds for the Amber LED (!) to appear, then power-cycle the drive shelf to set shelf ID. |

3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
4. Turn on the power switches to both nodes.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=a
905e56e-c995-4704-9673-adfa0005a891" width="711"> </iframe></div>
```

Animation - Turn on the power to the controllers




ⓘ Initial booting may take up to eight minutes.

5. Assign an initial node management IP address to one of the nodes.

| If the management network has DHCP… | Then… |
|---|---|
| Configured | Record the IP address assigned to the new controllers. |

| If the management network has DHCP… | Then… |
| --- | --- |
| Not configured | a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment.<br>Check your laptop or console's online help if you do not know how to configure PuTTY.<br>b. Enter the management IP address when prompted by the script. |

6. Using System Manager on your laptop or console, configure your cluster:
   a. Point your browser to the node management IP address.

      The format for the address is https://x.x.x.x.

   b. Configure the system using the data you collected in the ONTAP Configuration Guide .
7. Set up your account and download Active IQ Config Advisor:
   a. Log in to your existing account or create an account.

      NetApp Support Registration

   b. Register your system.

      NetApp Product Registration

   c. Download Active IQ Config Advisor.

      NetApp Downloads: Config Advisor
8. Verify the health of your system by running Config Advisor.
9. After you have completed the initial configuration, go to the ONTAP & ONTAP System Manager Documentation Resources page for information about configuring additional features in ONTAP.

## Maintain

### Add an I/O module - FAS9500

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 take over 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.

#### Option 1: Add the I/O module to a system with open slots

You can add an I/O module into an empty module slot in your system as either a NIC or a storage module for the SAS storage shelves.

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 take over 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 the open position.
   c. Remove the blanking cover.
4. Install the I/O module:
   a. Align the I/O module with the edges of the slot.
   b. Slide 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.
   c. Push the I/O cam latch all the way up to lock the module in place.
5. If the replacement I/O module is a NIC, cable the module to the data switches.

   > Make sure that any unused I/O slots have blanks installed to prevent possible thermal issues.

6. Reboot the node from the LOADER prompt: *bye*
7. Give back 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. If you are using slots 3 and/or 7 for networking, use the `storage port modify -node <node name> -port <port name> -mode network` command to convert the slot for networking use.
10. Repeat these steps for controller B.
11. If you installed a storage I/O module, install and cable your SAS shelves, as described in Hot-adding a SAS shelf.

#### Option 2: Add an I/O module in a system with no open slots

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

1. If you are:

| Replacing a… | Then… |
|---|---|
| NIC I/O module with the same the same number of ports | The LIFs will automatically migrate when its controller module is shut down. |
| NIC I/O module with fewer ports | 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. |
| NIC I/O module with a storage I/O module | 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 take over 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.

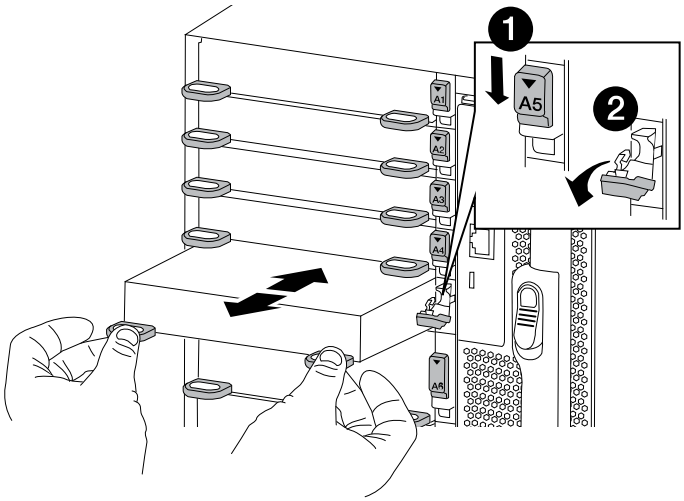
      The cam button moves away from the chassis.
   b. Rotate the cam latch down until it is in a horizontal position.

      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.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=09
03b1f9-187b-4bb8-9548-ae9b0012bb21" width="711"> </iframe></div>
```

      Animation - Replacing an I/O module




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

6. Install the I/O module into the target slot:
   a. Align the I/O module with the edges of the slot.
   b. Slide 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.
   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. If the replacement I/O module is a NIC, cable the module or modules to the data switches.
9. Reboot the node from the LOADER prompt: *bye*
10. Give back 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:

| If I/O module is a… | Then… |
|---|---|
| NIC module in slots 3 or 7, | Use the `storage port modify -node *<node name> -port *<port name> -mode network` command for each port. |
| Storage module | Install and cable your SAS shelves, as described in Hot-adding a SAS shelf. |

13. Repeat these steps for controller B.

## Boot media

### Replace the boot media - FAS9500

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.

### Pre-shutdown checks for onboard encryption keys - FAS9500

Prior to shutting down the impaired controller and checking the status of the onboard encryption keys, you must check the status of the impaired controller, disable automatic giveback, and check the version of ONTAP that is running.

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 the NetApp Encryption overview with the CLI.

#### Steps

1. Check the status of the impaired controller:
   - If the impaired controller is at the login prompt, log in as `admin`.
   - If the impaired controller is at the LOADER prompt and is part of HA configuration, log in as `admin` on the healthy controller.
   - If the impaired controller is in a standalone configuration and at LOADER prompt, contact mysupport.netapp.com.
2. 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`

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:
   - If <lno-DARE> or <1Ono-DARE> is displayed in the command output, the system does not support NVE, proceed to shut down the controller.

**ONTAP 9.6 and later**

Before shutting down the impaired controller, you need to verify whether the system has either NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) enabled. If so, you need to verify the configuration.

1. Verify whether NVE is in use for any volumes in the cluster: `volume show -is-encrypted true`

   If any volumes are listed in the output, NVE is configured and you need to verify the NVE configuration. If no volumes are listed, check whether NSE is configured and in use.

2. Verify whether NSE is configured and in use: `storage encryption disk show`
   - If the command output lists the drive details with Mode & Key ID information, NSE is configured and you need to verify the NSE configuration and in use.
   - If no disks are shown, NSE is not configured.
   - If NVE and NSE are not configured, no drives are protected with NSE keys, it's safe to shut down the impaired controller.

**Verify NVE configuration**

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
  1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
     a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
     b. Enter the command to display the key management information: `security key-manager onboard show-backup`
     c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

d. Return to admin mode: `set -priv admin`

e. Shut down the impaired controller.

2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:

   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.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`

   c. Shut down the impaired controller.

3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:

   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      > Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`

   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.

   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`

   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

   f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

   g. Return to admin mode: `set -priv admin`

   h. You can safely shut down the controller.

### Verify NSE configuration

1. Display the key IDs of the authentication keys that are stored on the key management servers: `security key-manager key-query -key-type NSE-AK`

   > After the ONTAP 9.6 release, you may have additional key manager types. The types are `KMIP`, `AKV`, and `GCP`. The process for confirming these types is the same as confirming `external` or `onboard` key manager types.

- If the `Key Manager` type displays `external` and the `Restored` column displays `yes`, it's safe to shut down the impaired controller.

- If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.
- If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`, you need to complete some additional steps.

1. If the `Key Manager` type displays `onboard` and the `Restored` column displays `yes`, manually back up the OKM information:
   a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   b. Enter the command to display the key management information: `security key-manager onboard show-backup`
   c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
   d. Return to admin mode: `set -priv admin`
   e. You can safely shut down the controller.
2. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager external sync`

      If the command fails, contact NetApp Support.

      mysupport.netapp.com

   b. Verify that the `Restored` column equals `yes` for all authentication keys: `security key-manager key-query`
   c. You can safely shut down the controller.
3. If the `Key Manager` type displays `onboard` and the `Restored` column displays anything other than `yes`:
   a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`

      Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.

      mysupport.netapp.com

   b. Verify the `Restored` column shows `yes` for all authentication keys: `security key-manager key-query`
   c. Verify that the `Key Manager` type shows `onboard`, and then manually back up the OKM information.
   d. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
   e. Enter the command to display the key management backup information: `security key-manager onboard show-backup`

f. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.

g. Return to admin mode: `set -priv admin`

h. You can safely shut down the controller.

#### Shut down the impaired controller - FAS9500

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

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

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |

| If the impaired controller is displaying… | Then… |
| --- | --- |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### Remove the controller, replace the boot media, and transfer the boot image - FAS9500

## You must remove and open the controller module, locate and replace the boot media in the controller, and then transfer the image to the replacement boot media.

### Step 1: Remove the controller module

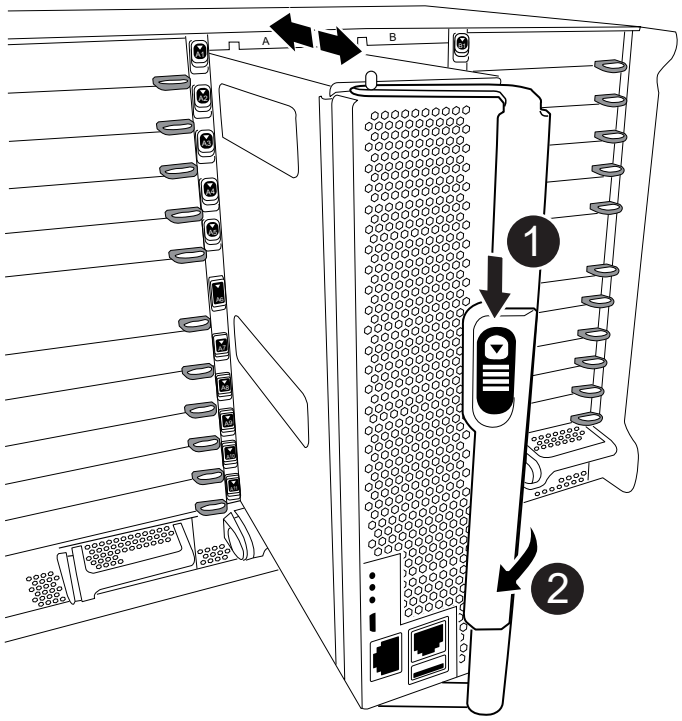
To access components inside the controller, you must first remove the controller module from the system and then remove the cover on the controller module.

#### 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 terra cotta button on the cam handle downward until it unlocks.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=5e029
a19-8acc-4fa1-be5d-ae78004b365a" width="711"> </iframe></div>
```

Animation - Remove controller module

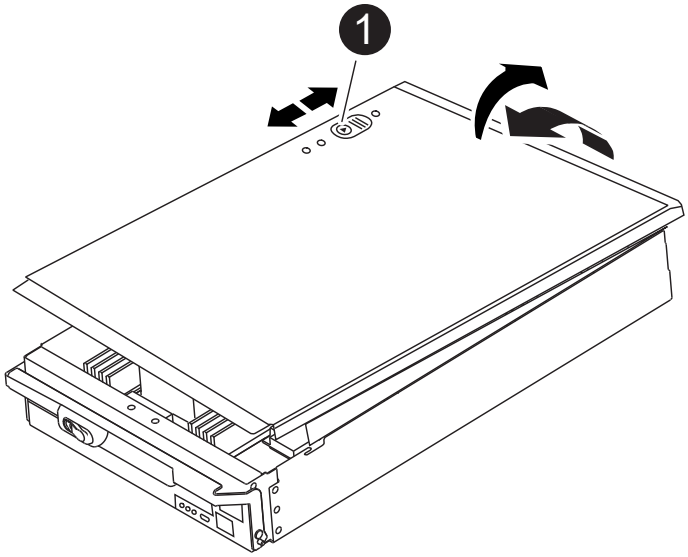



| | |
|---|---|
| 1 | Cam handle release button |
| 2 | Cam handle |

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.



| | |
|---|---|
| ❶ | Controller module cover locking button |

### Step 2: Replace the boot media

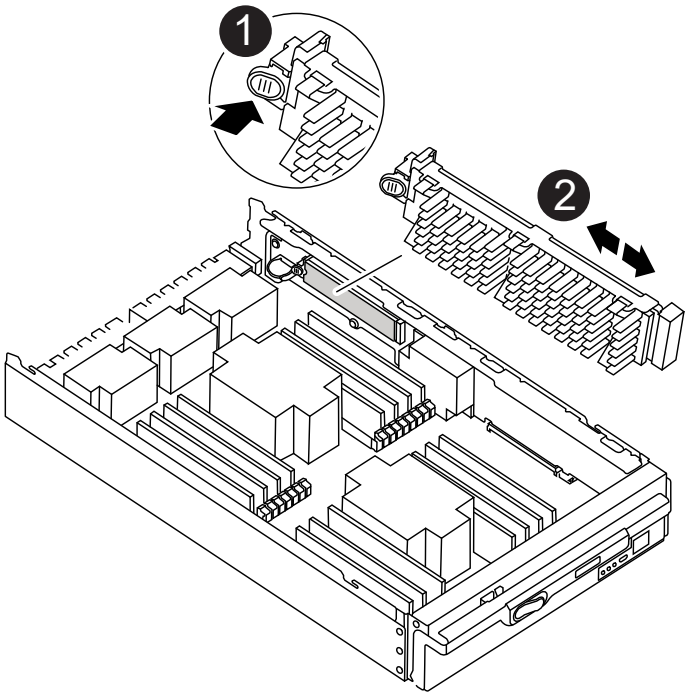
You must locate the boot media in the controller and follow the directions to replace it.

#### 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:

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=16df4
90c-f94f-498d-bb04-ae78004b3781" width="711"> </iframe></div>
```

Animation - Replace boot media




| | |
|---|---|
| ❶ | Press release tab |
| ❷ | 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. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

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

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

#### Before you begin

- 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. Although the environment variables and bootargs are retained, you should check that all required boot environment variables and bootargs are properly set for your system type and configuration using the `printenv bootarg name` command and correct any errors using the `setenv variable-name <value>` command.

a. Check the boot environment variables:
   - bootarg.init.boot_clustered
   - partner-sysid
   - bootarg.init.flash_optimized for AFF
   - bootarg.init.san_optimized for AFF
   - bootarg.init.switchless_cluster.enable
b. If External Key Manager is enabled, check the bootarg values, listed in the `kenv` ASUP output:
   - bootarg.storageencryption.support <value>
   - bootarg.keymanager.support <value>
   - kmip.init.interface <value>
   - kmip.init.ipaddr <value>
   - kmip.init.netmask <value>
   - kmip.init.gateway <value>
c. If Onboard Key Manager is enabled, check the bootarg values, listed in the `kenv` ASUP output:
   - bootarg.storageencryption.support <value>
   - bootarg.keymanager.support <value>
   - bootarg.onboard_keymanager <value>
d. Save the environment variables you changed with the `savenv` command
e. Confirm your changes using the `printenv variable-name` command.

7. 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.

8. 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 iniitator adapter_name`

   c. Halt to return to Maintenance mode: `halt`

   The changes will be implemented when the system is booted.

#### Boot the recovery image - FAS9500

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

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 | a. Press `y` when prompted to restore the backup configuration.<br>b. Press `y` when prompted to overwrite `/etc/ssh/ssh_host_ecdsa_key`.<br>c. Press `y` when prompted to confirm if the restore backup was successful.<br>d. Press `Y` when prompted to the restored configuration copy.<br>e. Set the healthy node to advanced privilege level: `set -privilege advanced`<br>f. Run the restore backup command: `system node restore-backup -node local -target-address impaired_node_IP_address`<br>g. Return the node to admin level: `set -privilege admin`<br>h. Press `y` when prompted to use the restored configuration.<br>i. Press `y` when prompted to reboot the node. |

| If your system has… | Then… |
| --- | --- |
| No network connection | a. Press `n` when prompted to restore the backup configuration.<br>b. Reboot the system when prompted by the system.<br>c. Select the **Update flash from backup config** (sync flash) option from the displayed menu.<br><br>If you are prompted to continue with the update, press `y`. |
| No network connection and is in a MetroCluster IP configuration | a. Press `n` when prompted to restore the backup configuration.<br>b. Reboot the system when prompted by the system.<br>c. Wait for the iSCSI storage connections to connect.<br><br>You can proceed after you see the following messages:<br><br>`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).`<br>`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).`<br>`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).`<br>`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).`<br><br>d. Select the **Update flash from backup config** (sync flash) option from the displayed menu.<br><br>If you are prompted to continue with the update, press `y`. |

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 `setenvenvironment_variable_name changed_value` command.

d. Save your changes using the `saveenv` command.

5. The next depends on your system configuration:
   - If your system has onboard keymanager, NSE or NVE configured, go to Post boot media replacement steps for OKM, NSE, and NVE
   - 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.<br>b. Confirm the target node is ready for giveback with the `storage failover show` 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.

#### Post boot media replacement steps for OKM, NSE, and NVE - FAS9500

## Once environment variables are checked, you must complete steps specific to restore Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) and NetApp Volume Encryption (NVE).

1. Determine which section you should use to restore your OKM, NSE, or NVE configurations: If NSE or NVE are enabled along with Onboard Key Manager you must restore settings you captured at the beginning of this procedure.
   - If NSE or NVE are enabled and Onboard Key Manager is enabled, go to Restore NVE or NSE when Onboard Key Manager is enabled.
   - If NSE or NVE are enabled for ONTAP 9.6, go to Restore NSE/NVE on systems running ONTAP 9.6 and later.

### Restore NVE or NSE when Onboard Key Manager is enabled

1. Connect the console cable to the target node.
2. Use the `boot_ontap` command at the LOADER prompt to boot the node.
3. Check the console output:

| If the console displays… | Then… |
|---|---|
| The LOADER prompt | Boot the node to the boot menu: `boot_ontap menu` |
| Waiting for giveback…. | a. Enter `Ctrl-C` at the prompt<br>b. At the message: Do you wish to halt this node rather than wait [y/n]? , enter: `y`<br>c. At the LOADER prompt, enter the `boot_ontap menu` command. |

4. At the Boot Menu, enter the hidden command, `recover_onboard_keymanager`, and reply `y` at the prompt.
5. Enter the passphrase for the onboard key manager you obtained from the customer at the beginning of this procedure.
6. When prompted to enter the backup data, paste the backup data you captured at the beginning of this section, when asked. Paste the output of `security key-manager backup show` OR `security key-manager onboard show-backup` command.

   The data is output from either `security key-manager backup show` or security key-manager onboard show-backup` command.

   Example of backup data:

   Enter the backup data:

```
-------------------------BEGIN BACKUP-------------------------
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAAACQAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.
.
.
.
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA

-------------------------END BACKUP-------------------------
```


7. At the Boot Menu select the option for Normal Boot.

   The system boots to Waiting for giveback… prompt.

8. Move the console cable to the partner node and log in as admin.
9. Confirm the target node is ready for giveback with the `storage failover show` command.
10. Give back only the CFO aggregates with the `storage failover giveback -fromnode local -only-cfo-aggregates true` command.
    - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
    - If the command fails because of an open CIFS session, check with the customer how to close out CIFS sessions.

      > Terminating CIFS can cause loss of data.

    - If the command fails because the partner "not ready", wait 5 minutes for the NVRAMs to synchronize.
    - If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate content for more information.
11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and storage failover show-giveback commands.

    Only the CFO aggregates (root aggregate and CFO style data aggregates) will be shown.

12. If you are running ONTAP 9.6 or later, run the security key-manager onboard sync:
    a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
    b. Enter the `security key-manager key-query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication

keys.

> If the `Restored` column = anything other than `yes/true`, contact Customer Support.

c. Wait 10 minutes for the key to synchronize across the cluster.

13. Move the console cable to the partner node.
14. Give back the target node using the `storage failover giveback -fromnode local` command.
15. Check the giveback status, three minutes after it reports complete, using the `storage failover show` command.

    If giveback is not complete after 20 minutes, contact Customer Support.

16. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home node and port.

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

17. Move the console cable to the target node and run the `version -v` command to check the ONTAP versions.
18. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

**Restore NSE/NVE on systems running ONTAP 9.6 and later**

1. Connect the console cable to the target node.
2. Use the `boot_ontap` command at the LOADER prompt to boot the node.
3. Check the console output:

| If the console displays… | Then… |
|---|---|
| The login prompt | Go to step 7. |
| Waiting for giveback… | a. Log into the partner node.<br>b. Confirm the target node is ready for giveback with the `storage failover show` command. |

4. Move the console cable to the partner node and give back the target node storage using the `storage failover giveback -fromnode local -only-cfo-aggregates true local` command.
   - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in the slot until a replacement is received.
   - If the command fails because of an open CIFS sessions, check with customer how to close out CIFS sessions.

     > Terminating CIFS can cause loss of data.

   - If the command fails because the partner is "not ready", wait 5 minutes for the NVMEMs to

synchronize.

- If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate content for more information.

5. Wait 3 minutes and check the failover status with the `storage failover show` command.
6. At the clustershell prompt, enter the `net int show -is-home false` command to list the logical interfaces that are not on their home node and port.

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

7. Move the console cable to the target node and run the `version -v` command to check the ONTAP versions.
8. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
9. Use the `storage encryption disk show` at the clustershell prompt, to review the output.
10. Use the `security key-manager key-query` command to display the encryption and authentication keys that are stored on the key management servers.
    - If the `Restored` column = `yes/true`, you are done and can proceed to complete the replacement process.
    - If the `Key Manager type` = `external` and the `Restored` column = anything other than `yes/true`, use the `security key-manager external restore` command to restore the key IDs of the authentication keys.

      If the command fails, contact Customer Support.

    - If the `Key Manager type` = `onboard` and the `Restored` column = anything other than `yes/true`, use the `security key-manager onboard sync` command to re-sync the Key Manager type.

      Use the `security key-manager key-query` command to verify that the `Restored` column = `yes/true` for all authentication keys.

11. Connect the console cable to the partner node.
12. Give back the node using the `storage failover giveback -fromnode local` command.
13. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.

#### Return the failed part to NetApp - FAS9500

Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Hot-swap a caching module - FAS9500

The NVMe SSD FlashCache modules (FlashCache or caching modules) are located in the front of the NVRAM11 module in Slot 6 of FAS9500 systems. You can hot-swap the caching module of the same capacity from the same or different supported vendor.

If you need to or want to cold-swap the FlashCache module, follow the procedures for replacing an I/O module.

**Before you begin**

Your storage system must meet certain criteria depending on your situation:

- It must have the appropriate operating system for the caching module you are installing.
- The caching module must be functioning well enough to be seen by the system. If the caching module is not functioning since the last boot, you cannot use this procedure and must use the cold-swap procedure.
- It must support the caching capacity.
- The replacement caching module must have the same capacity as the failed caching module, but can be from a different supported vendor.
- All other components in the storage system must be functioning properly; if not, you must contact technical support.

**Steps**

1. If you are not already grounded, properly ground yourself.
2. Locate the failed caching module, in slot 6, by the lit amber Attention LED on the front of the caching module.
3. Prepare the caching module slot for replacement as follows:

   a. Record the caching module capacity, part number, and serial number on the target node: `system node run local sysconfig -av 6`

   b. In admin privilege level, prepare the target NVMe slot for removal, responding `y` when prompted whether to continue: `system controller slot module remove -node node_name -slot slot_number` The following command prepares slot 6-1 on node1 for removal, and displays a message that it is safe to remove:

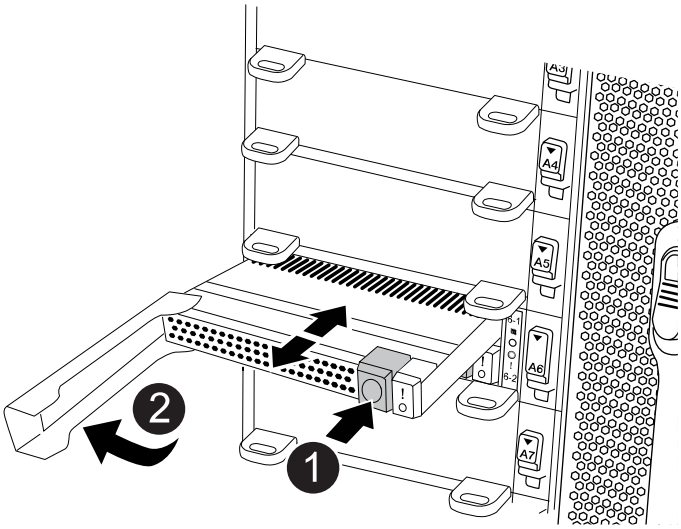
   ```
   ::> system controller slot module remove -node node1 -slot 6-1

   Warning: SSD module in slot 6-1 of the node node1 will be powered off
   for removal.
   Do you want to continue? (y|n): `y`

   The module has been successfully removed from service and powered
   off. It can now be safely removed.
   ```

   c. Display the slot status with the `system controller slot module show` command.

   The NVMe slot status displays `powered-off` in the screen output for the caching module that needs replacing.

   See the Command man pages for your version of ONTAP for more details.

4. Remove the caching module:




| | |
|---|---|
| 1 | Terra cotta release button. |
| 2 | Caching module cam handle. |

a. Press the terra cotta release button on the front of the caching module.

> Do not use the numbered and lettered I/O cam latch to eject the caching module. The numbered and lettered I/O cam latch ejects the entire NVRAM11 module and not the caching module.

b. Rotate the cam handle until the caching module begins to slide out of the NVRAM11 module.

c. Gently pull the cam handle straight toward you to remove the caching module from the NVRAM11 module.

   Be sure to support the caching module as you remove it from the NVRAM11 module.

5. Install the caching module:

   a. Align the edges of the caching module with the opening in the NVRAM11 module.

   b. Gently push the caching module into the bay until the cam handle engages.

   c. Rotate the cam handle until it locks into place.

6. Bring the replacement caching module online by using the `system controller slot module insert` command as follows:

   The following command prepares slot 6-1 on node1 for power-on, and displays a message that it is powered on:

```
::> system controller slot module insert -node node1 -slot 6-1

Warning: NVMe module in slot 6-1 of the node localhost will be powered
on and initialized.
Do you want to continue? (y|n): `y`

The module has been successfully powered on, initialized and placed into
service.
```

7. Verify the slot status using the `system controller slot module show` command.

   Make sure that command output reports status for the as `powered-on` and ready for operation.

8. Verify that the replacement caching module is online and recognized, and then visually confirm that the amber attention LED is not lit: `sysconfig -av slot_number`

   > If you replace the caching module with a caching module from a different vendor, the new vendor name is displayed in the command output.

9. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

## Chassis

### Replace the chassis - FAS9500

#### Before you begin

To replace the chassis, you must remove the power supplies, fans, controller modules, I/O modules, DCPM modules, and USB LED module from the impaired chassis, remove the impaired chassis from the equipment rack or system cabinet, install the replacement chassis in its place, and then install the components into the replacement chassis.

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

#### About this task

- 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.

### Shutdown the impaired controller - FAS9500

You must shut down the controller or controller in the chassis prior to moving them to the new chassis.

#### About this task

- If you have a cluster with more than two controllers, 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 the Administration overview with the CLI.
- 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`

**Steps**

1. If your system has two controller modules, disable the HA pair.

| If your system is running clustered ONTAP with… | Then… |
|---|---|
| Two controllers in the cluster | `cluster ha modify -configured false` `storage failover modify -node node0 -enabled false` |
| More than two controllers in the cluster | `storage failover modify -node node0 -enabled false` |

2. Halt the controller, pressing `y` when you are prompted to confirm the halt: `system node halt -node` *`node_name`*

   The confirmation message looks like the following:

```
Warning: This operation will cause controller "node-name" to be marked
as unhealthy. Unhealthy nodes do not participate in quorum voting. If
the controller goes out of service and one more controller goes out of
service there will be a data serving failure for the entire cluster.
This will cause a client disruption. Use "cluster show" to verify
cluster state. If possible bring other nodes online to improve the
resiliency of this cluster.

Do you want to continue? {y|n}:
```

   You must perform a clean system shutdown before replacing the chassis to avoid losing unwritten data in the nonvolatile memory (NVMEM/NVRAM). Depending on your system, if the NVMEM/NVRAM LED is flashing, there is content in the NVMEM/NVRAM that has not been saved to disk. You need to reboot the controller and start from the beginning of this procedure. If repeated attempts to cleanly shut down the controller fail, be aware that you might lose any data that was not saved to disk.

3. Where applicable, halt the second controller to avoid a possible quorum error message in an HA pair configuration: `system node halt -node` *`second_node_name`* `-ignore-quorum-warnings true -skip-lif-migration-before-shutdown true`

   Answer `y` when prompted.

To replace the chassis, you must remove the components from the old chassis and install them in the replacement chassis.

### Step 1: Remove the power supplies

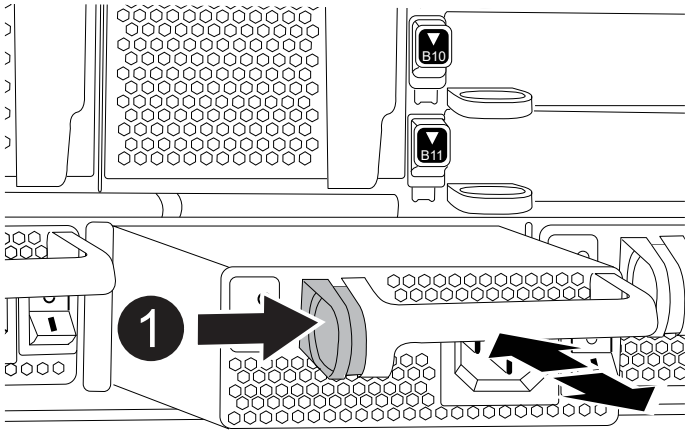
Removing the power supplies when replacing a chassis involves turning off, disconnecting, and then removing the power supply from the old chassis.

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 terra cotta 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.

   ```
   <div class="aspect-ratio"><iframe frameborder="1" height="400"
   scrolling="auto"
   src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=590b3
   414-6ea5-42b2-b7f4-ae78004b86a4" width="711"> </iframe></div>
   ```

   Animation - Remove/install PSU




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

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

### Step 2: Remove the fans

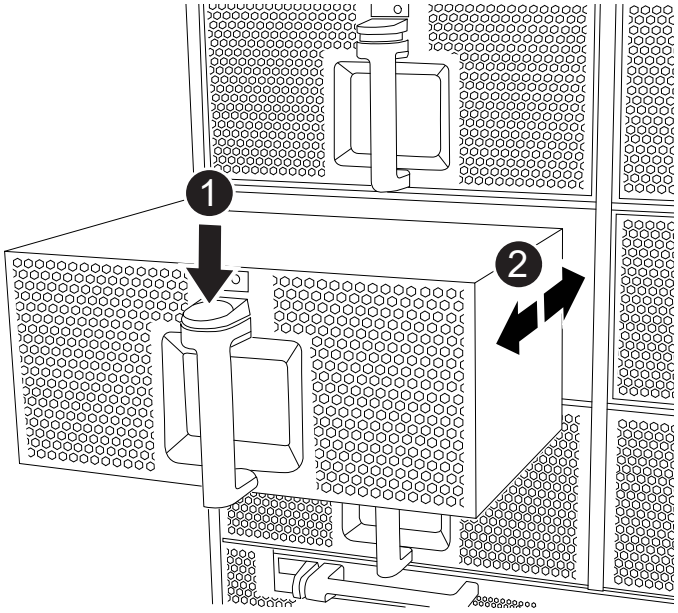
To remove the fan modules when replacing the chassis, you must perform a specific sequence of tasks.

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. Press the terra cotta 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.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=86b0e
d39-1083-4b3a-9e9c-ae78004c2ffc" width="711"> </iframe></div>
```

Animation - Remove/install fan




| | |
|---|---|
| 1 | Terra cotta release button |
| 2 | Slide fan in/out of chassis |

4. Set the fan module aside.
5. 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.

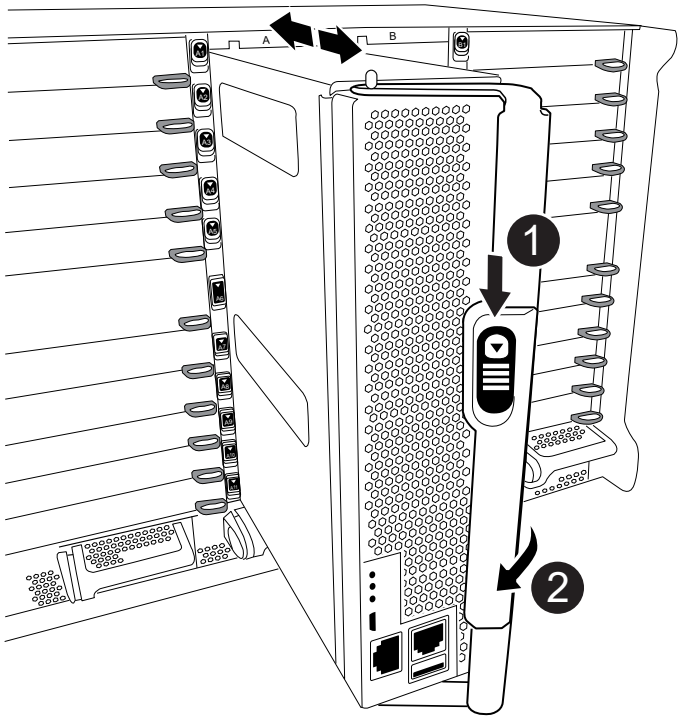
1. If you are not already grounded, properly ground yourself.
2. Unplug the cables from the impaired controller module, and keep track of where the cables were

connected.

3. Slide the terra cotta button on the cam handle downward until it unlocks.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=5e029
a19-8acc-4fa1-be5d-ae78004b365a" width="711"> </iframe></div>
```

Animation - Remove controller module




| | |
|---|---|
| 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. 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

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 FlashCache module, if present, from the NVRAM module when moving it to a new chassis.

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.

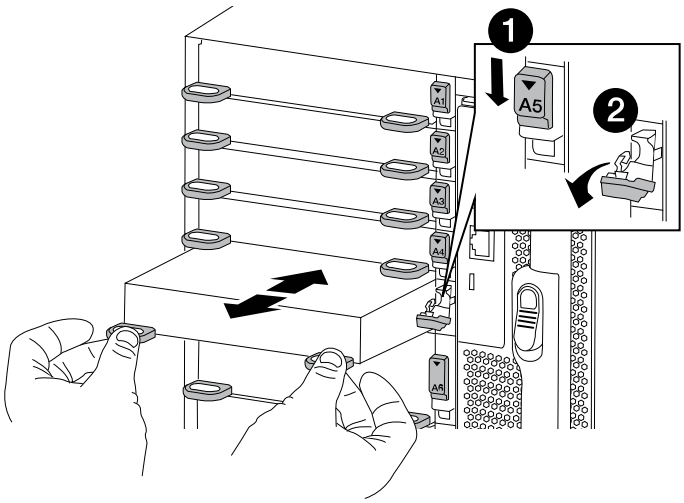
      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

   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.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=09
03b1f9-187b-4bb8-9548-ae9b0012bb21" width="711"> </iframe></div>
```

      Animation - Remove/install I/O module




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

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

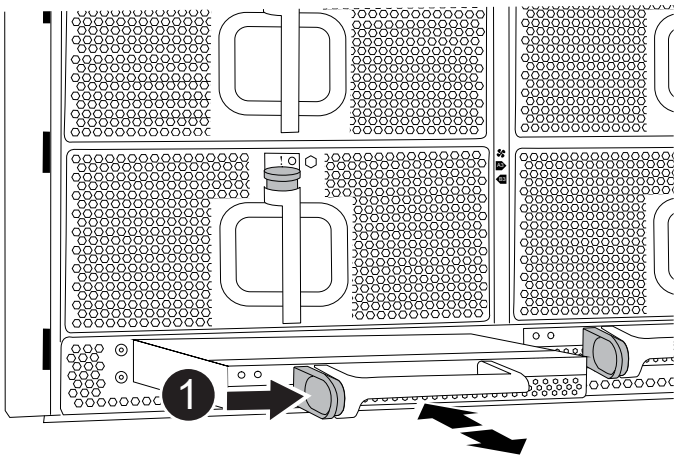
### Step 5: Remove the De-stage Controller Power Module

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

1. If you are not already grounded, properly ground yourself.
2. Press the terra cotta locking button on the module handle, and then slide the DCPM module out of the chassis.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=c067c
f9d-35b8-4fbe-9573-ae78004c2328" width="711"> </iframe></div>
```

Animation - Remove/install DCPM




| | |
|---|---|
| 1 | DCPM module terra cotta locking button |

3. 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

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.

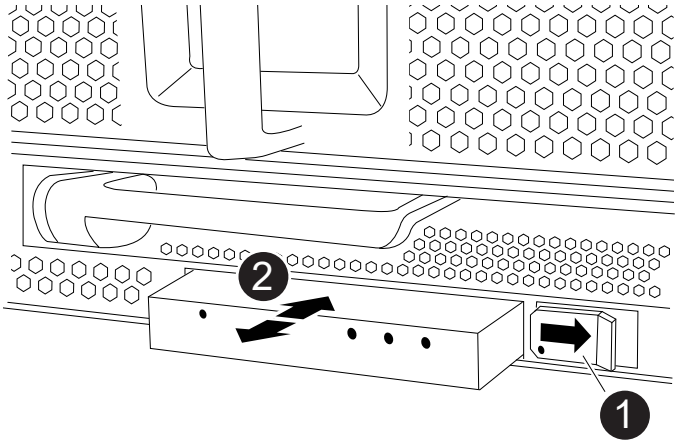
5. Slide the chassis all the way into the equipment rack or system cabinet.
6. Secure the front of the chassis to the equipment rack or system cabinet, using the screws you removed from the old chassis.
7. Secure the rear of the chassis to the equipment rack or system cabinet.
8. If you are using the 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

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.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=bc46a3e
8-6541-444e-973b-ae78004bf153" width="711"> </iframe></div>
```

Animation - Remove/install USB module




| | |
|---|---|
| 1 | Eject the module. |
| 2 | Slide out of 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

Once the replacement chassis is installed into the rack or system cabinet, you must reinstall the de-stage

controller power modules into it.

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

3. Repeat this step for the remaining DCPM module.

**Step 9: Install fans into the chassis**

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

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

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

**Step 10: Install I/O modules**

To install I/O modules, including the NVRAM/FlashCache 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. If you are not already grounded, properly ground yourself.
2. 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.
3. Recable the I/O module, as needed.
4. 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**

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

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

3. 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.

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

**Step 12: Install the controller**

After you install the controller module and any other components into the new chassis, boot it to a state where you can run the interconnect diagnostic test.

1. If you are not already grounded, properly ground yourself.
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 console to the controller module, and then reconnect the management port.
4. Connect the power supplies to different power sources, and then turn them on.
5. 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.

6. Repeat the preceding steps to install the second controller into the new chassis.
7. 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.

## To complete the chassis replacement, you must complete specific tasks.

### 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.

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
      - non-ha

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

### Step 2: Run system-level diagnostics

After installing a new chassis, you should run interconnect diagnostics.

**Before you begin**

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

1. If the node to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the node boots to Maintenance mode, halt the node: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      > During the boot process, you can safely respond `y` to prompts:

2. Repeat the previous step on the second node if you are in an HA configuration.

   > Both controllers must be in Maintenance mode to run the interconnect test.

3. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

   The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

   You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

7. Proceed based on the result of the preceding step.

| If the system-level diagnostics tests… | Then… |
| --- | --- |
| Were completed without any failures | a. Clear the status logs: `sldiag device clearstatus`<br>b. Verify that the log was cleared: `sldiag device status`<br>The following default response is displayed:<br>`SLDIAG: No log messages are present.`<br>c. Exit Maintenance mode on both controllers: `halt`<br>The system displays the LOADER prompt.<br>You must exit Maintenance mode on both controllers before proceeding any further.<br>d. Enter the following command on both controllers at the LOADER prompt: `bye`<br>e. Return the node to normal operation. |

| If your system is running ONTAP… | Then… |
| --- | --- |
| With two nodes in the cluster | Issue these commands: `node::> cluster ha modify -configured true`<br>`node::> storage failover modify -node node0 -enabled true` |

| If your system is running ONTAP… | Then… |
| --- | --- |
| With more than two nodes in the cluster | Issue this command: `node::> storage failover modify -node node0 -enabled true` |
| In a stand-alone configuration | You have no further steps in this particular task.<br>You have completed system-level diagnostics. |
| Resulted in some test failures | Determine the cause of the problem.<br>a. Exit Maintenance mode: `halt`<br>b. Perform a clean shutdown, and then disconnect the power supplies.<br>c. Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Reconnect the power supplies, and then power on the storage system.<br>e. Rerun the system-level diagnostics test. |

#### 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 & Replacements page for further information.

### Controller module

#### Replace the controller module - FAS9500

To replace the impaired controller module, you must shut down the impaired controller, move the internal components to the replacement controller module, install the replacement controller module, and reboot the replacement controller.

#### Before you begin

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 is a FlexArray system or 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 node - FAS9500

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### Replace the controller module hardware - FAS9500

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.

The following animation shows the whole process of moving components from the impaired to the replacement controller.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=dc8d4ac
b-e061-45dd-8a0e-ae78004b6974" width="711"> </iframe></div>
```

Animation - Remove controller module

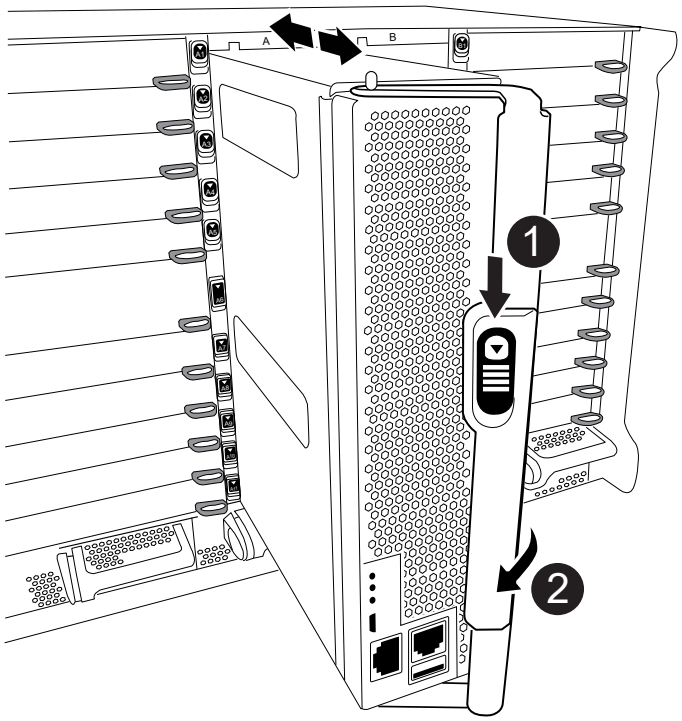
#### Step 1: Remove the controller module

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.

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 terra cotta button on the cam handle downward until it unlocks.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=5e029
a19-8acc-4fa1-be5d-ae78004b365a" width="711"> </iframe></div>
```

Animation - Remove controller module

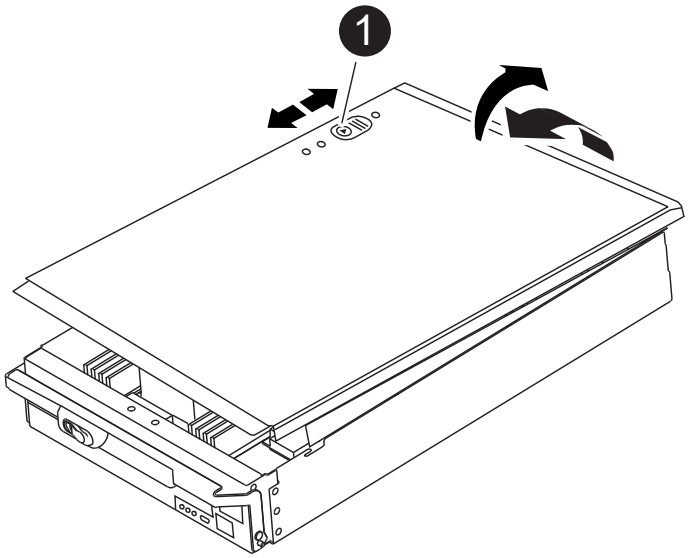



| | |
|---|---|
| 1 | Cam handle release button |
| 2 | Cam handle |

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.

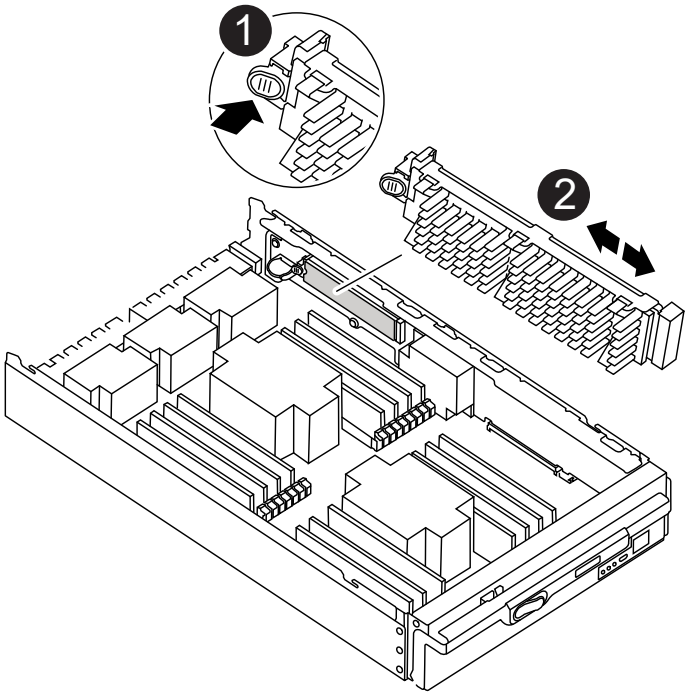



| | |
|---|---|
| 1 | Controller module cover locking button |

**Step 2: 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.

1. 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 reseat it into the socket.

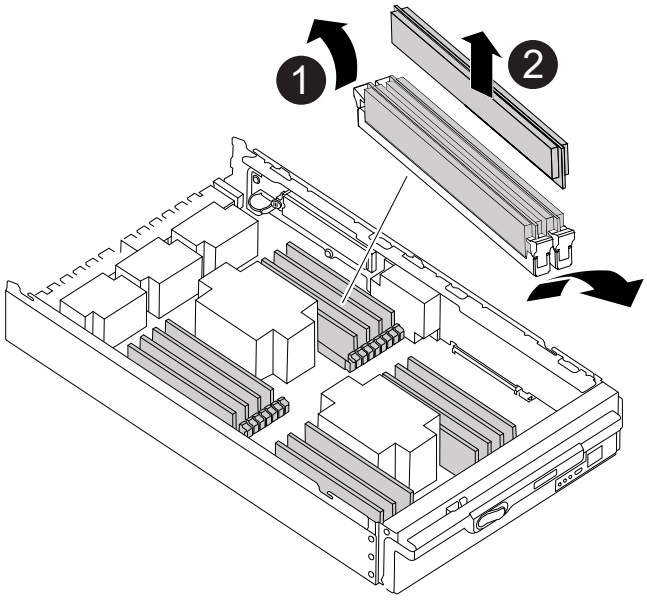
5. Push the boot media down to engage the locking button on the boot media housing.

**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.

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 |

| | |
|---|---|
| ❷ | 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 replacement controller module, you must install the replacement controller module into the system chassis and boot the operating system.

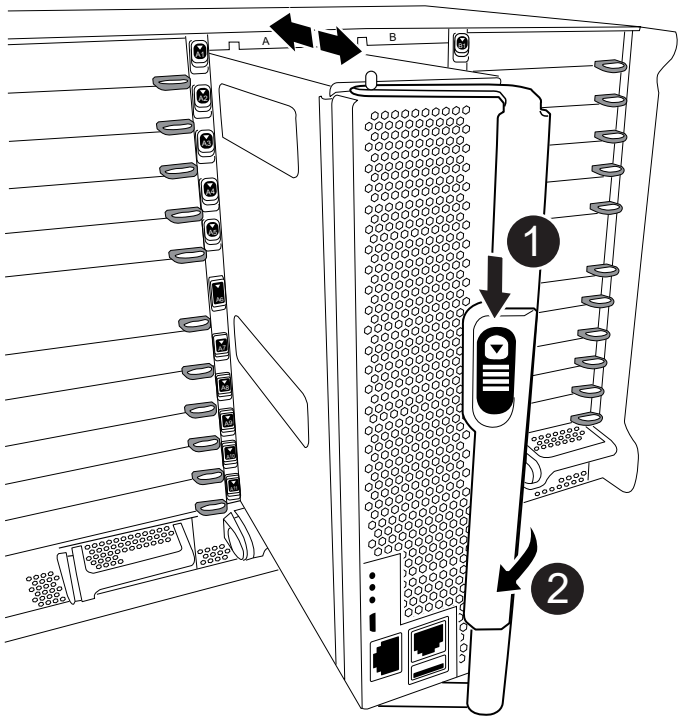
For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

> 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.

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.

   ```
   <div class="aspect-ratio"><iframe frameborder="1" height="400"
   scrolling="auto"
   src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=f2aa1
   4b4-0d95-4109-b410-ae78004b35c9" width="711"> </iframe></div>
   ```

   Animation - Install controller module




| | |
|---|---|
| 1 | Cam handle release button |
| 2 | Cam handle |

> 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.

   > 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 controller module cam handle to 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 LOADER.

# After completing the hardware replacement, you verify the low-level system configuration of the replacement controller, reconfigure system settings as necessary, and then run system-level diagnostics.

## Step 1: Set and verify the system time after replacing the controller module

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: `show date`

   The date and time are given in GMT.

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 HA state of the controller module

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

1. In Maintenance mode from the replacement controller module, verify that all components display the same `HA` state: `ha-config show`

| If your system is in… | The HA state for all components should be… |
|---|---|
| An HA pair | ha |
| A MetroCluster FC configuration with four or more nodes | mcc |

| If your system is in… | The HA state for all components should be… |
| --- | --- |
| A MetroCluster IP configuration | mccip |

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

### Step 3: Run system-level diagnostics

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

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

1. If the node to be serviced is not at the LOADER prompt, reboot the node: `halt`

   After you issue the command, you should wait until the system stops at the LOADER prompt.

2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to function properly: `boot_diags`

   During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

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

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

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

| If you want to run diagnostic tests on… | Then… |
| --- | --- |
| Individual components | a. Clear the status logs: `sldiag device clearstatus`<br>b. Display the available tests for the selected devices: `sldiag device show -dev dev_name`<br><br>dev_name can be any one of the ports and devices identified in the preceding step.<br><br>c. Examine the output and, if applicable, select only the tests that you want to run: `sldiag device modify -dev dev_name -selection only`<br><br>-selection only disables all other tests that you do not want to run for the device.<br><br>d. Run the selected tests: `sldiag device run -dev dev_name`<br><br>After the test is complete, the following message is displayed:<br><br>`*> <SLDIAG:_ALL_TESTS_COMPLETED>`<br><br>e. Verify that no tests failed: `sldiag device status -dev dev_name -long -state failed`<br><br>System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component. |

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

5. Proceed based on the result of the preceding step:

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

| If your node is in… | Then… |
| --- | --- |
| An HA pair | Perform a give back: `storage failover giveback -ofnode replacement_node_name`<br>If you disabled automatic giveback, re-enable it with the storage failover modify command. |

| If your node is in… | Then… |
| --- | --- |
| Resulted in some test failures | Determine the cause of the problem:<br>a. Exit Maintenance mode: `halt`<br>After you issue the command, wait until the system stops at the LOADER prompt.<br>b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis.<br>Leave the power supplies turned on to provide power to the other controller module.<br>c. Verify that you have observed all the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>d. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu.<br>The controller module boots up when fully seated.<br>e. Select Boot to maintenance mode from the menu.<br>f. Exit Maintenance mode by entering the following command: `halt`<br>After you issue the command, wait until the system stops at the LOADER prompt.<br>g. Rerun the system-level diagnostic test. |

#### Recable the system - FAS9500

## Continue the replacement procedure by recabling the storage and network conigurations.

### Step 1: Recable the system

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

#### Steps

1. Recable the system.
2. Verify that the cabling is correct by using Active IQ Config Advisor.
   a. Download and install Config Advisor.
   b. Enter the information for the target system, and then click Collect Data.
   c. Click the Cabling tab, and then examine the output. Make sure that all disk shelves are displayed and all disks appear in the output, correcting any cabling issues you find.
   d. Check other cabling by clicking the appropriate tab, and then examining the output from Config Advisor.

The system ID and disk assignment information reside in the NVRAM module, which is in a module separate from the controller module and not impacted by the controller module replacement.

**Step 2: Reassign disks**

If the storage system is in an HA pair, the system ID of the new controller module is automatically assigned to the disks when the giveback occurs at the end of the procedure. 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
                                       Takeover
   Node              Partner           Possible     State Description
   ------------      ------------      --------
   -------------------------------------
   node1             node2             false        System ID changed on
   partner (Old:
                                                     151759755, New:
   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.

      For more information, see the Manual giveback commands topic to override the veto.

   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 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

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.

  For more information, see Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration topic.

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`

#### Complete system restoration - FAS9500

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.

#### 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.

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

   NetApp Support

   > 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.

**Steps**

1. Install each license key: `system license add -license-code license-key, license-key...`
2. 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: Restore Storage and Volume Encryption functionality

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

**Step**

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use 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

### Step 3: Verify LIFs and registering the serial number

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

**Steps**

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

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

2. Register the system serial number with NetApp Support.

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

#### 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 & Replacements page for further information.

### Replace a DIMM - FAS9500

You must replace a DIMM in the controller module when your system registers an increasing number of correctable error correction codes (ECC); failure to do so causes a system panic.

#### Before you begin

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 node

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

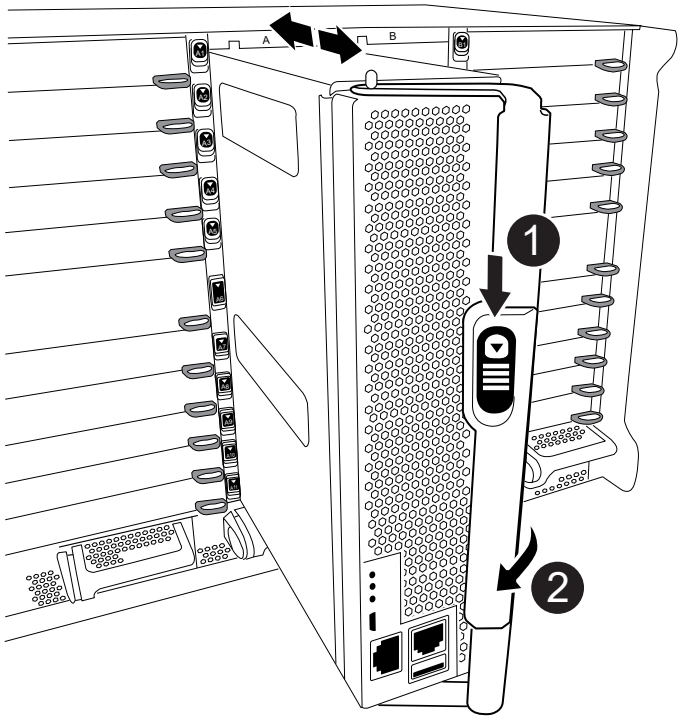
#### Step 2: Remove the controller module

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.

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 terra cotta button on the cam handle downward until it unlocks.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=5e029
a19-8acc-4fa1-be5d-ae78004b365a" width="711"> </iframe></div>
```

Animation - Remove controller module

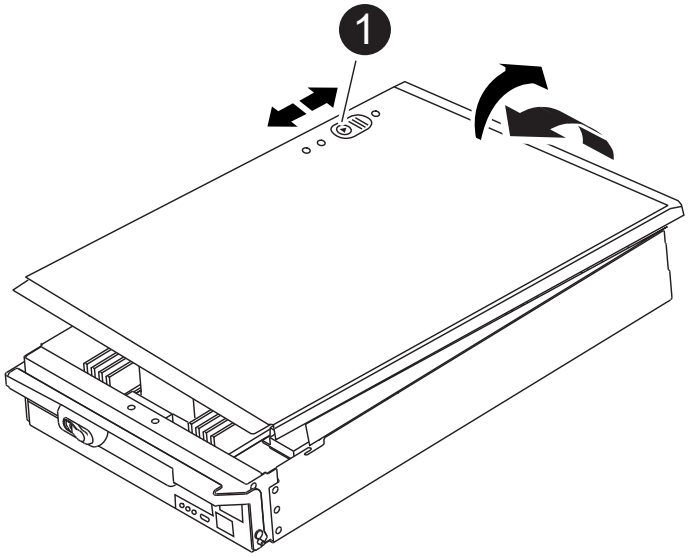



| | |
|---|---|
| 1 | Cam handle release button |
| 2 | Cam handle |

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.



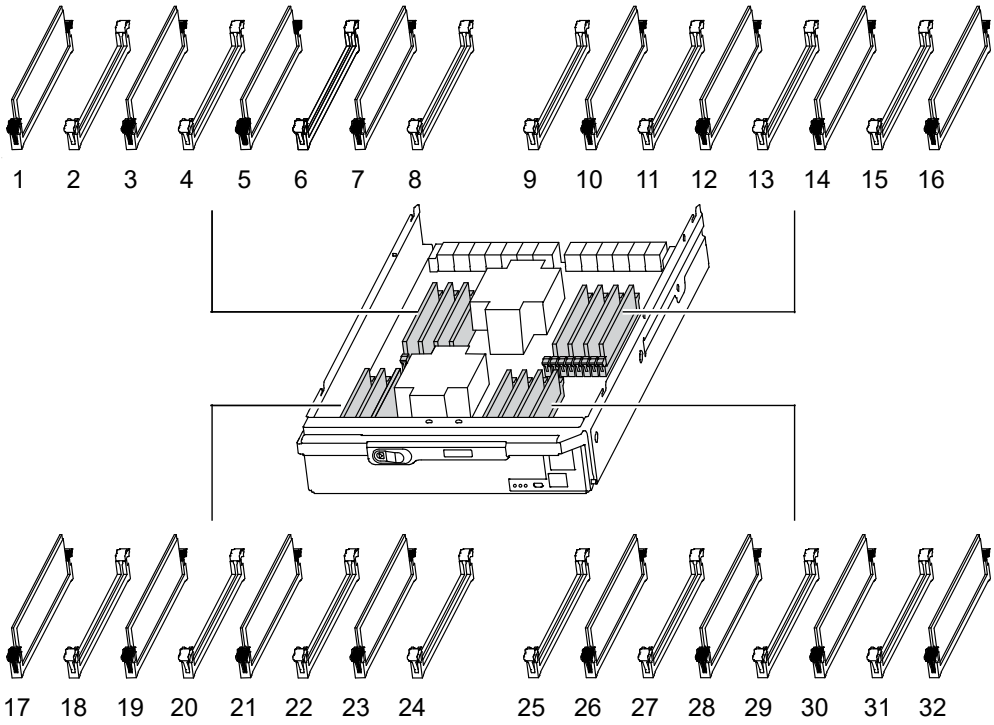
| | |
|---|---|
| ❶ | Controller module cover locking button |

**Step 3: Replace the DIMMs**

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

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

> Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty blinks every two seconds.

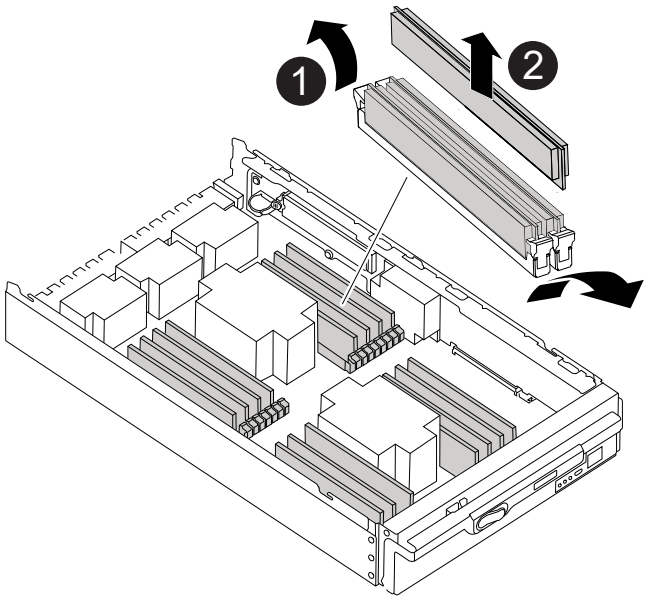



3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.

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

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=d62a4
c7c-8296-4d60-9981-ae78004b36f7" width="711"> </iframe></div>
```

Animation - Replace DIMM




| | |
|---|---|
| 1 | DIMM ejector tabs |
| 2 | DIMM |

4. 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.

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

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

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

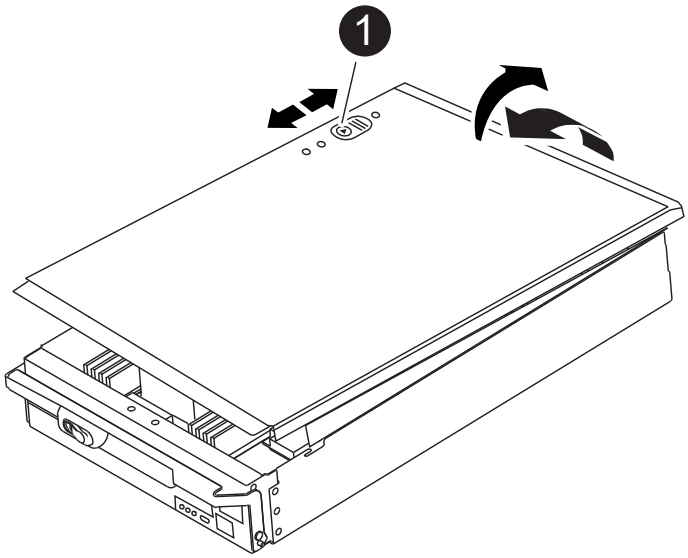
6. Push carefully, but firmly, on the top edge of the DIMM until the ejector tabs snap into place over the notches at the ends of the DIMM.
7. Close the controller module cover.

#### 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.

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.

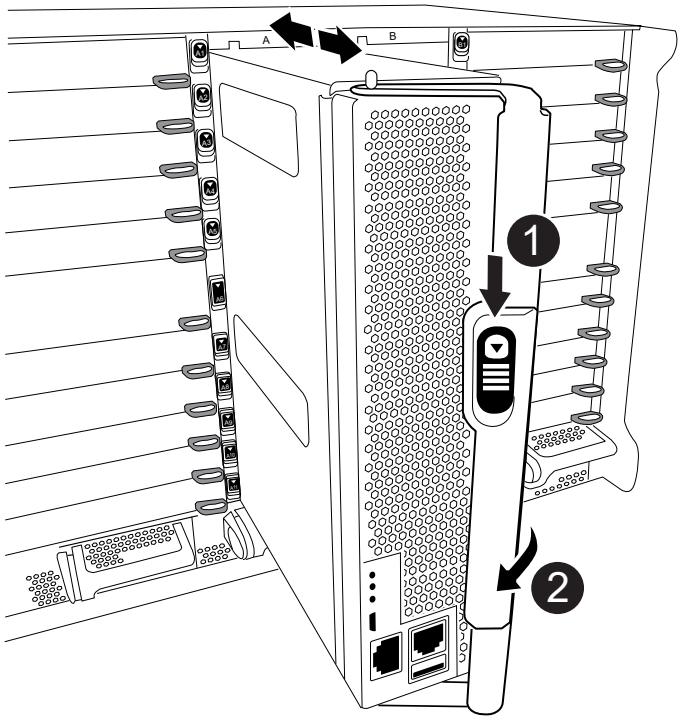


| | |
|---|---|
| 1 | Controller module cover locking button |

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.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=f2aa1
4b4-0d95-4109-b410-ae78004b35c9" width="711"> </iframe></div>
```

Animation - Install controller



| | |
|---|---|
| ❶ | Cam handle release button |
| ❷ | Cam handle |

> 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.

#### Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

Your system must be at the LOADER prompt to start System Level Diagnostics.

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

1. If the node to be serviced is not at the LOADER prompt, perform the following steps:
   a. Select the Maintenance mode option from the displayed menu.
   b. After the node boots to Maintenance mode, halt the node: `halt`

      After you issue the command, you should wait until the system stops at the LOADER prompt.

      > During the boot process, you can safely respond `y` to prompts.

      - If a prompt appears warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy node remains down.
2. At the LOADER prompt, access the special drivers specifically designed for system-level diagnostics to

function properly: `boot_diags`

During the boot process, you can safely respond `y` to the prompts until the Maintenance mode prompt (*>) appears.

3. Run diagnostics on the system memory: `sldiag device run -dev mem`
4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

   System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.

5. Proceed based on the result of the preceding step:

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

| If your node is in… | Then… |
|---|---|
| An HA pair | Perform a give back: `storage failover giveback -ofnode replacement_node_name`<br>If you disabled automatic giveback, re-enable it with the storage failover modify command. |

| If your node is in… | Then… |
| --- | --- |
| Resulted in some test failures | Determine the cause of the problem:<br>a. Exit Maintenance mode: `halt`<br>After you issue the command, wait until the system stops at the LOADER prompt.<br>b. Verify that you have observed all the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.<br>c. Boot the controller module you are servicing, interrupting the boot by pressing `Ctrl-C` when prompted to get to the Boot menu:<br>◦ If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis.<br>The controller module boots up when fully seated.<br>◦ If you have one controller module in the chassis, connect the power supplies, and then turn them on.<br>d. Select Boot to maintenance mode from the menu.<br>e. Exit Maintenance mode by entering the following command: `halt`<br>After you issue the command, wait until the system stops at the LOADER prompt.<br>f. Rerun the system-level diagnostic test. |

#### 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 & Replacements page for further information.

### Replace the Destage Control Power Module containing the NVRAM11 battery - FAS9500

To hot-swap a de-stage controller power module (DCPM), which contains the NVRAM11 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.

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.

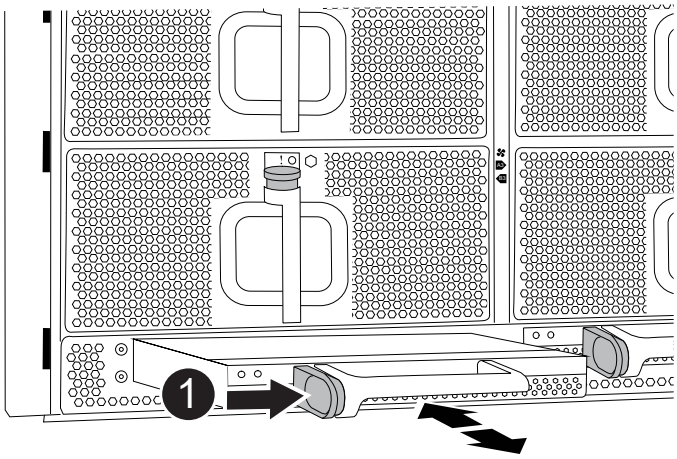
   The LED will be steady amber if the module is faulty.

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

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

   ```
   <div class="aspect-ratio"><iframe frameborder="1" height="400"
   scrolling="auto"
   src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=c067c
   f9d-35b8-4fbe-9573-ae78004c2328" width="711"> </iframe></div>
   ```

   Animation - Remove/install DCPM




| | |
|---|---|
| 1 | DCPM module terra cotta 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 Amber LED flashes four times upon insertion and the green LED also flashes if the battery is providing a voltage. If it does not flash, it will likely need to be replaced.

#### 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.

Safety Information and Regulatory Notices

#### 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 & Replacements page for further information.

### Swap out a fan - FAS9500

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.

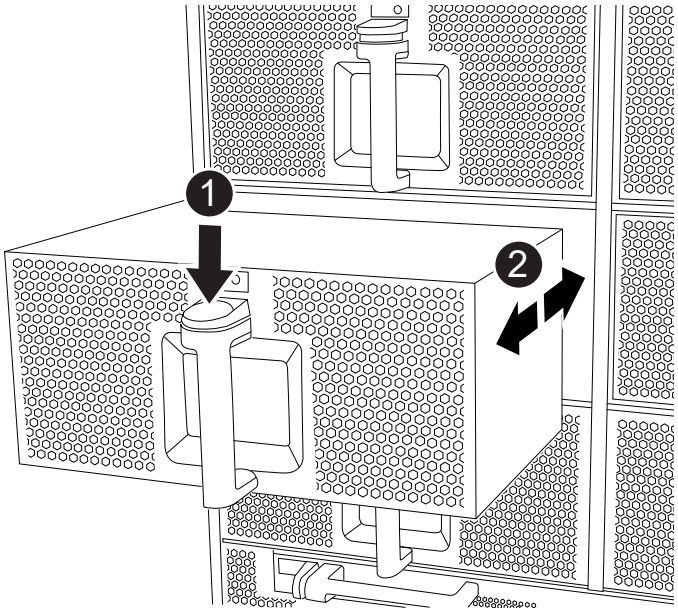
#### Steps

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 terra cotta 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.

   ```
   <div class="aspect-ratio"><iframe frameborder="1" height="400"
   scrolling="auto"
   src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=86b0e
   d39-1083-4b3a-9e9c-ae78004c2ffc" width="711"> </iframe></div>
   ```

   Animation - Remove/install fan




| | |
|---|---|
| 1 | Terra cotta release button |
| 2 | Slide fan in/out of chassis |

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 & Replacements page for further information.

## Replace an I/O module - FAS9500

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 node

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 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 the Administration overview with the CLI.

**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 `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### Step 2: Replace I/O modules

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

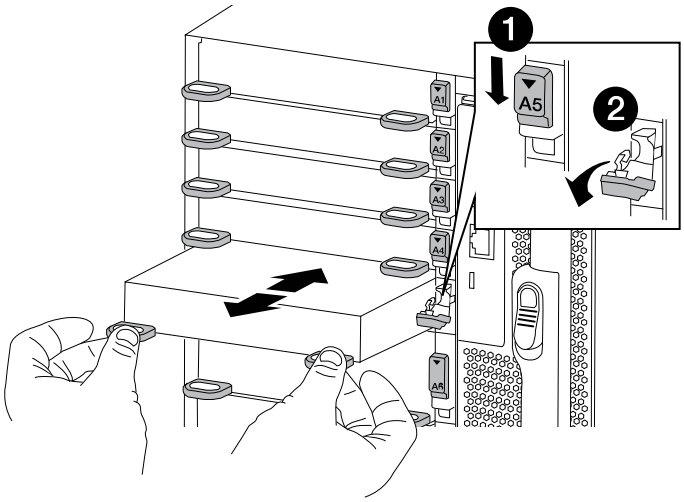
      The I/O module disengages from the chassis and moves about 1/2 inch out of the I/O slot.

   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.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=09
03b1f9-187b-4bb8-9548-ae9b0012bb21" width="711"> </iframe></div>
```

Animation - Remove/install I/O module




| | |
|---|---|
| 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.

1. From the LOADER prompt, reboot the node: *bye*
2. 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.

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

```
-giveback true
```

#### 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 & Replacements page for further information.

### Replace an LED USB module - FAS9500

The LED USB module provides connectivity to console ports and system status. Replacement of this module does not require tools and does not interrupt service.

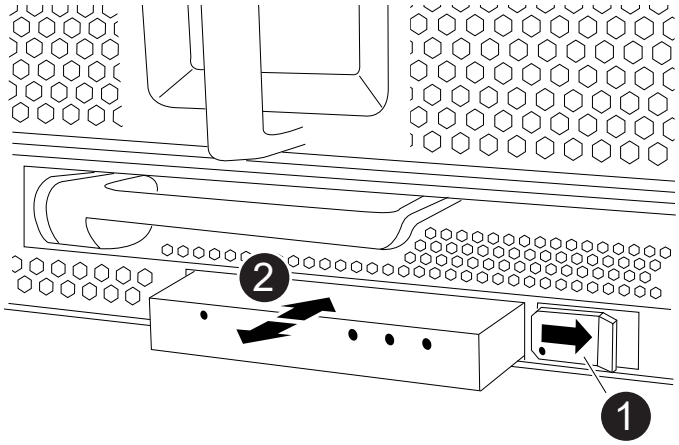
#### Step 1: Replace the LED USB module

**Steps**

1. Remove the old LED USB module:

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=bc46a
3e8-6541-444e-973b-ae78004bf153" width="711"> </iframe></div>
```

Animation - Remove/install LED-USB module




| | |
|---|---|
| 1 | Locking button |
| 2 | USB LED 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.

#### Step 2: Return the failed component

1. Return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

### Replace the NVRAM module and/or NVRAM DIMMs - FAS9500

The NVRAM module consists of the NVRAM11 and DIMMs. 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, move the DIMMs to the replacement module, and install the replacement NVRAM module into the chassis.

To replace and NVRAM DIMM, you must remove the NVRAM module from the chassis, replace the failed DIMM in the module, and then reinstall the NVRAM module.

#### About this task

Because the system ID is derived from the NVRAM module, if replacing the module, disks belonging to the system are reassigned to a 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 node

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 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 the Administration overview with the CLI.

#### 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 `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

#### 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.

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.

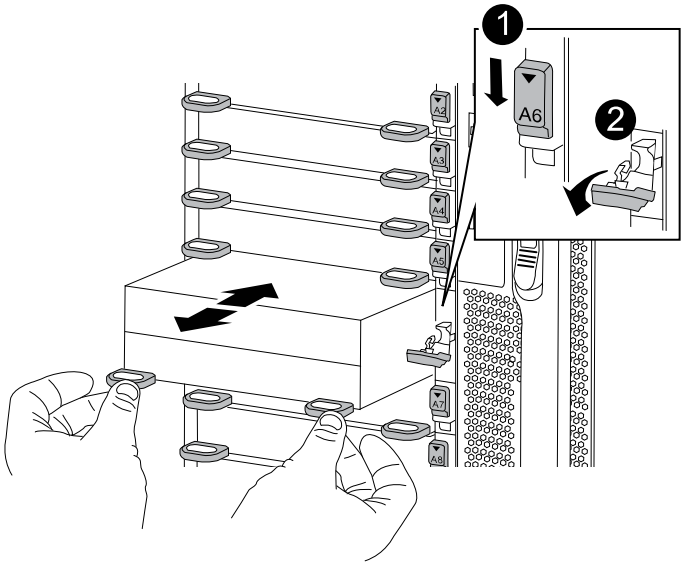
   b. Rotate the cam latch down until it is in a horizontal position.

      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.

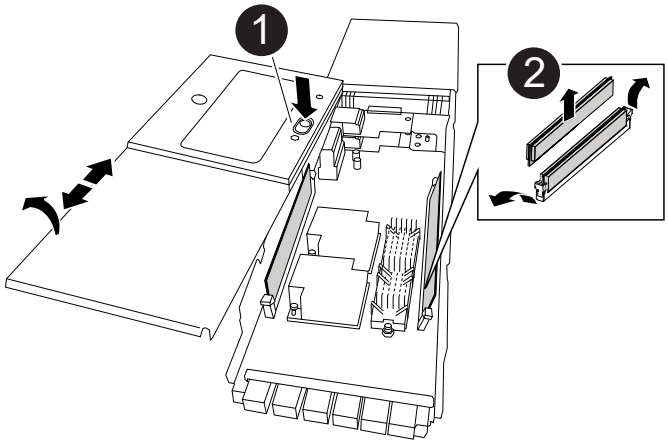
```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=22
8cbd14-4cb2-49b5-88f1-ae78004b9d84" width="711"> </iframe></div>
```

   Animation - Replace the NVRAM module




| | |
|---|---|
| 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. Remove the DIMMs, one at a time, from the old NVRAM module and install them in the replacement NVRAM module.
5. Close the cover on the module.
6. 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.

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.

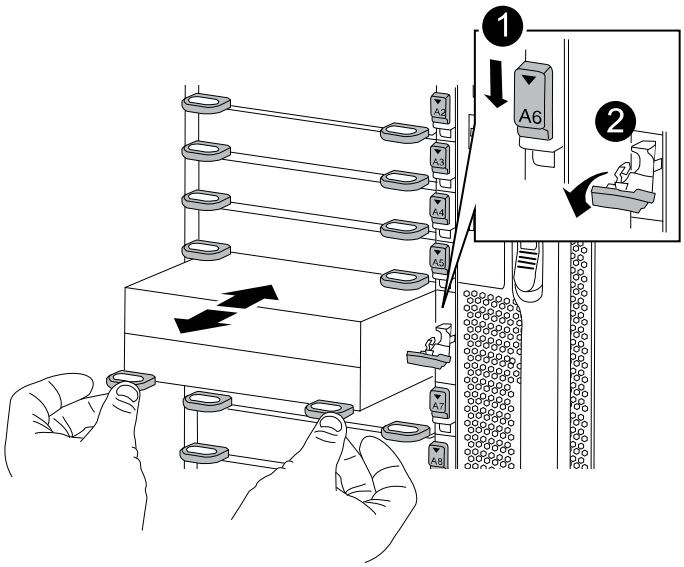
   b. Rotate the cam latch down until it is in a horizontal position.

      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.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=22
8cbd14-4cb2-49b5-88f1-ae78004b9d84" width="711"> </iframe></div>
```

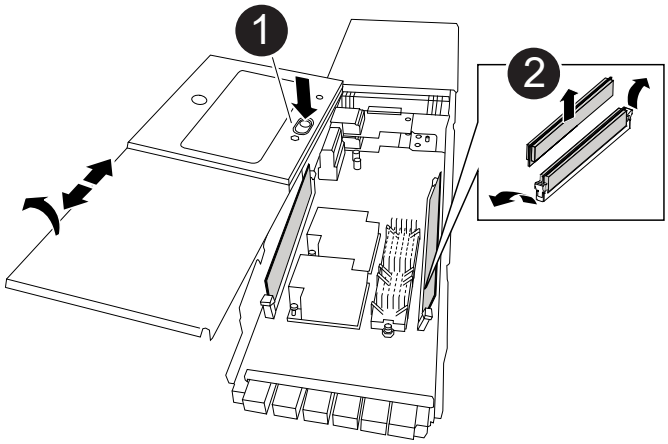
Animation - Replace the NVRAM module




| | |
|---|---|
| 1 | Lettered and numbered I/O cam latch |

| | |
|---|---|
| ❷ | 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.




| | |
|---|---|
| ❶ | Cover locking button |
| ❷ | 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.

   Each DIMM has an LED next to it that flashes when the DIMM has failed.

5. Install the replacement DIMM by aligning the DIMM with the socket and gently pushing the DIMM into the socket until the locking tabs lock in place.
6. Close the cover on the module.
7. Install the 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.

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

#### Step 5: Verify and set the HA state of the controller module

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

1. In Maintenance mode from the replacement controller module, verify that all components display the same

HA state: `ha-config show`

| If your system is in… | The HA state for all components should be… |
|---|---|
| An HA pair | ha |
| A MetroCluster FC configuration with four or more nodes | mcc |
| A MetroCluster IP configuration | mccip |

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

#### Step 6: Reassigning disks

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.

**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.
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`
                                    Takeover
Node              Partner           Possible     State Description
------------      ------------      --------
-------------------------------------
node1             node2             false        System ID changed on
partner (Old:
                                                 151759755, New:
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.

      For more information, see the Manual giveback commands topic to override the veto.

   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 Pool0
1.0.1  aggr0_1  node1 node1           1873775277 1873775277  -
1873775277 Pool0
.
.
.
```

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.

     See Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration for more information.

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`

#### Step 7: Restore Storage and Volume Encryption functionality

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

**Step**

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in NetApp Encryption overview with the CLI.
2. Use 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

#### Step 8: 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 & Replacements page for further information.

### Swap out a power supply - FAS9500

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.

**About this task**

- The power supplies are redundant and hot-swappable.
- 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.

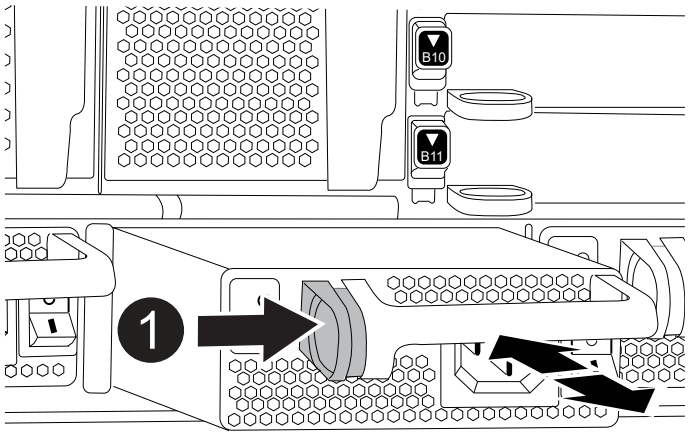
**Steps**

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 terra cotta 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.

   ```
   <div class="aspect-ratio"><iframe frameborder="1" height="400"
   scrolling="auto"
   src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=590b3
   414-6ea5-42b2-b7f4-ae78004b86a4" width="711"> </iframe></div>
   ```

   Animation - Remove/install PSU




| | |
|---|---|
| 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 & Replacements page for further information.

### Replace the real-time clock battery - FAS9500

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.

#### Step 1: Shut down the impaired node

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

  ONTAP 9 NetApp Encryption Power Guide

- If you have a SAN system, you must have checked event messages (`event log show`) for impaired controller SCSI blade.

  Each SCSI-blade process should be in quorum with the other nodes in the cluster. Any issues must be resolved before you proceed with the replacement.

- If you have a 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 the Administration overview with the CLI.
- 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 Remove controller module. |
| Waiting for giveback… | Press Ctrl-C, and then respond `y` when prompted. |
| System prompt or password prompt (enter system password) | Take over or halt the impaired controller from the healthy controller: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>When the impaired controller shows Waiting for giveback…, press Ctrl-C, and then respond `y`. |

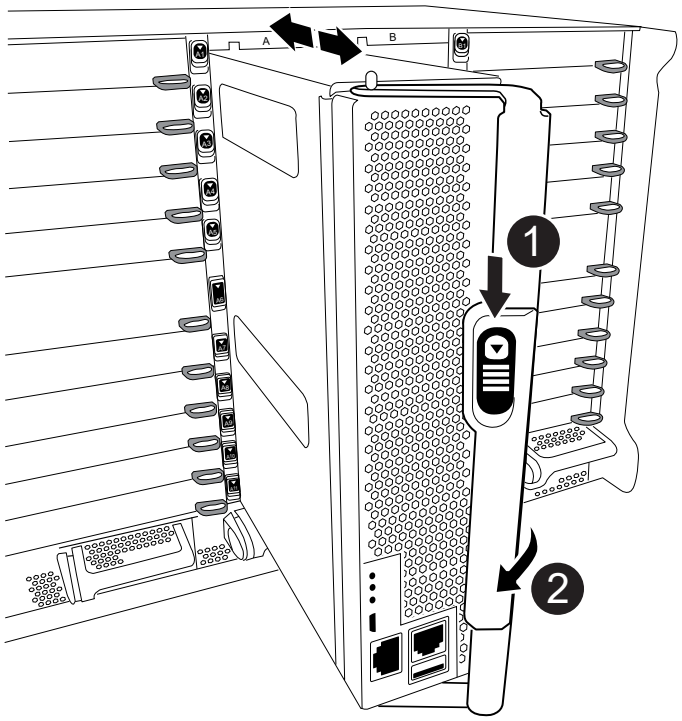
#### Step 2: Remove the controller

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.

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 terra cotta button on the cam handle downward until it unlocks.

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=5e029
a19-8acc-4fa1-be5d-ae78004b365a" width="711"> </iframe></div>
```

Animation - Remove controller module

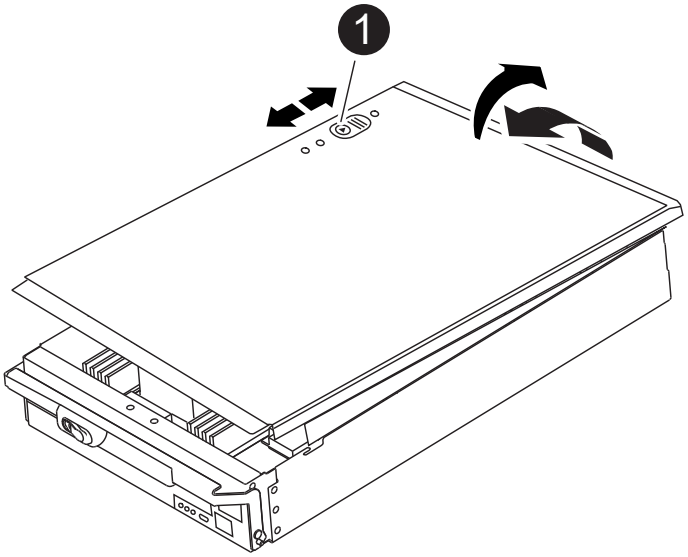



| | |
|---|---|
| 1 | Cam handle release button |
| 2 | Cam handle |

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 |

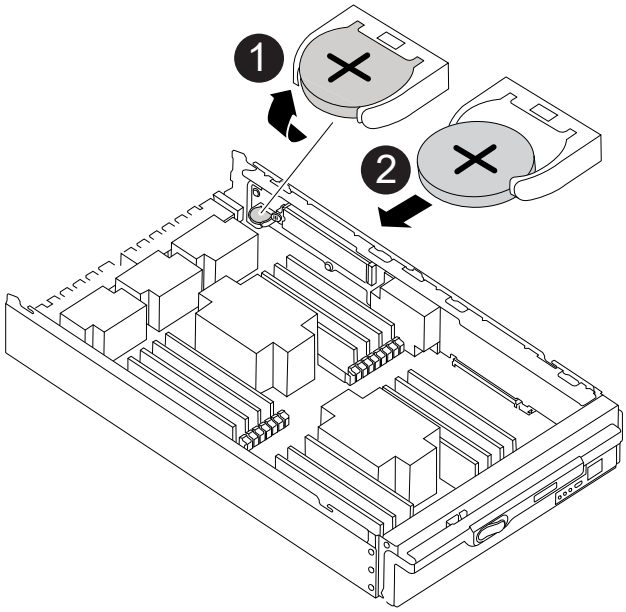
**Step 3: Replace the RTC battery**

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.

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

```
<div class="aspect-ratio"><iframe frameborder="1" height="400"
scrolling="auto"
src="https://netapp.hosted.panopto.com/Panopto/Pages/embed.aspx?id=3b977
f96-3ebb-4b11-9703-ae78004b4add" width="711"> </iframe></div>
```

Animation - Replace RTC battery




| | |
|---|---|
| 1 | Rotate battery up |
| 2 | Slide battery out from 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 the RTC battery, you must reinstall the controller module. If the RTC battery has been left out of the controller module for more than 10 minutes, you may have to reset the time and date.

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: 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 & Replacements page for further information.

**Copyright Information**

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

**Trademark Information**

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.