



C-Series systems

Install and maintain

NetApp
August 29, 2025

This PDF was generated from <https://docs.netapp.com/us-en/ontap-systems/asa-c250/install-setup.html> on August 29, 2025. Always check docs.netapp.com for the latest.

Table of Contents

- ASA C-Series systems 1
 - ASA C250 systems 1
 - Install and setup 1
 - Maintain 12
 - ASA C400 systems 96
 - Install and setup 96
 - Maintain 107
 - ASA C800 systems 220
 - Install and setup 220
 - Maintain 237

ASA C-Series systems

ASA C250 systems

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 - ASA C250

The Installation and Setup instructions give 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.



The ASA A250 and ASA C250 use the same installation procedure as the AFF A250 system.

[AFF A250 Installation and Setup Instructions](#)

Videos - ASA C250

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

[Animation - Installation and Setup of an AFF A250](#)



The ASA C250 uses the same installation procedure as the AFF A250 system.

Detailed steps - ASA C250

This section gives detailed step-by-step instructions for installing an ASA C250 system.

Step 1: Prepare for installation

To install your AFF A250 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.



Customers with specific power requirements must check HWU for their configuration options.

Before you begin

- Make sure you have access to the [NetApp Hardware Universe](#) (HWU) for information about site requirements.
- Make sure you have access to the [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. Set up your account:
 - a. Log in to your existing account or create an account.
 - b. [Register](#) 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;		Cluster interconnect network
	X66240-2 (112-00573), 2m		
	X66240A-2 (112-00598), 2m; X66240A-5 (112-00600), 5m		Data
100 GbE cable	X66211-2 (112-00574), 2m; X66211-5 (112-00576), 5m		Storage
RJ-45 (order dependent)	Not applicable		Management network (BMC and wrench port) and Ethernet data (e0a and e0b)

Type of cable...	Part number and length	Connector type	For...
Fibre Channel	X66250-2 (112-00342) 2m; X66250-5 (112-00344) 5m; X66250-15 (112-00346) 15m; X66250-30 (112-00347) 30m		
Micro-USB console cable	Not applicable		Console connection during software setup
Power cables	Not applicable		Powering up the system

6. Review the [ONTAP Configuration Guide](#) and collect the required information listed in that guide.

Step 2: Install the hardware

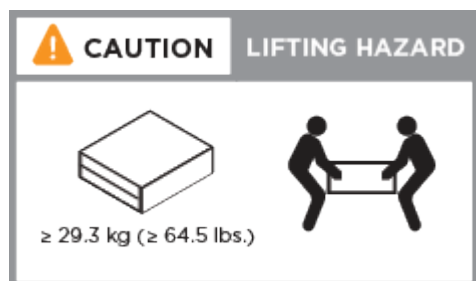
You need to install your system in a 4-post rack or NetApp system cabinet, as applicable.

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 to cluster

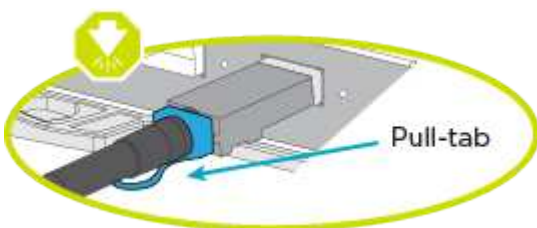
Cable the controllers to a cluster by using the two-node switchless cluster method or by using the cluster interconnect network method.

Option 1: 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.

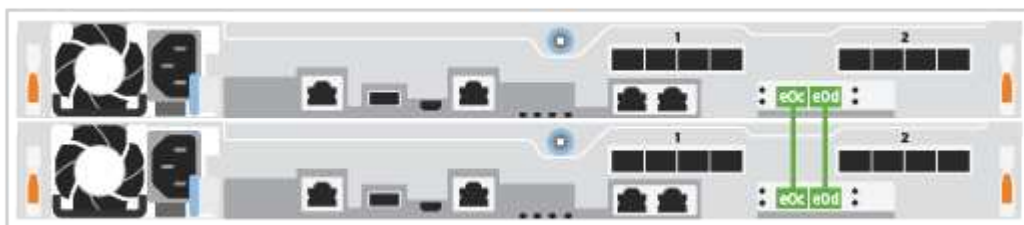
About this task

Use the animation or the tabulated steps to complete the cabling between the controllers and the switches. Perform the steps on each controller.

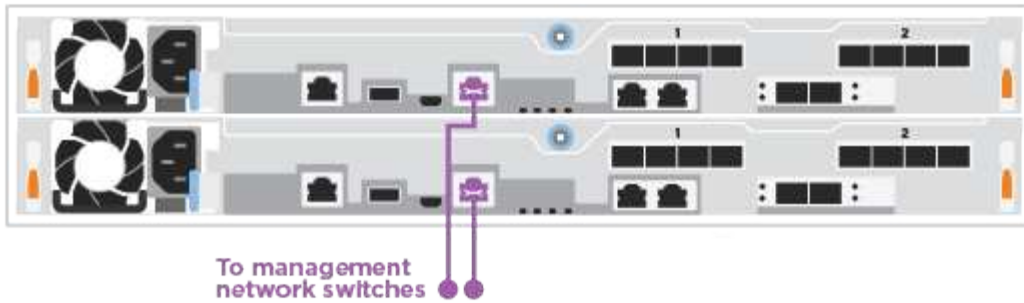
Animation - Cable two-node switchless cluster

Steps

1. Use the the 25GbE cluster interconnect cable to connect the cluster interconnect ports e0c to e0c and e0d to e0d.



2. Cable the wrench ports to the management network switches with the RJ45 cables.



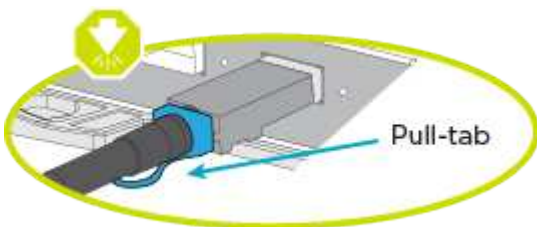
DO NOT plug in the power cords at this point.

Option 2: 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.

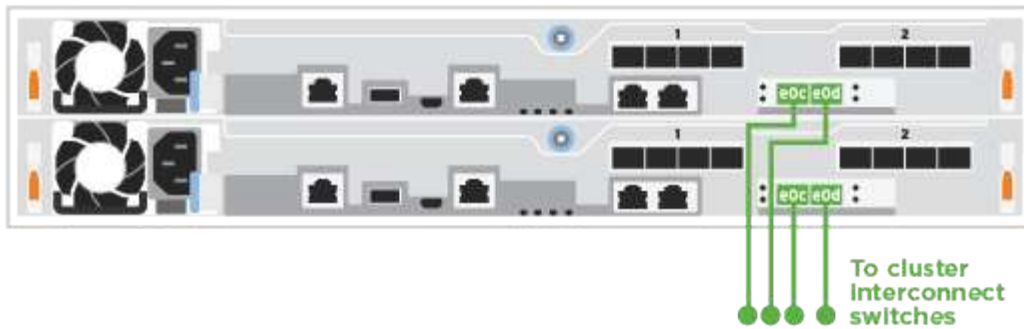
About this task

Use the animation or the steps to complete the cabling between the controllers and the switches. Perform the steps on each controller.

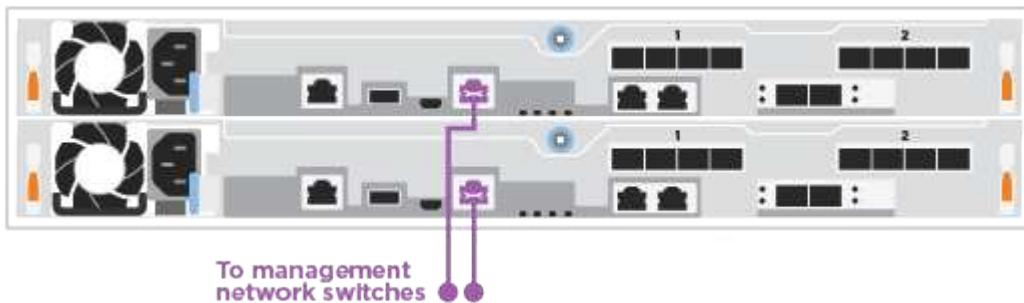
[Animation - Cable switched cluster](#)

Steps

1. Cable the cluster interconnect ports e0c and e0d to the 25 GbE cluster interconnect switches.



2. Cable the wrench ports to the management network switches with the RJ45 cables.



Step 4: Cable to host network or storage (Optional)

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.



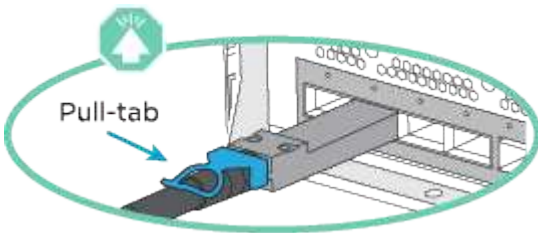
[NetApp Hardware Universe](#) slot priority for host network cards (Fibre Channel or 25GbE) is slot 2. However, if you have both cards, the Fibre Channel card goes in slot 2 and the 25GbE card goes in slot 1 (as shown in the options below). If you have an external shelf, the storage card goes in slot 1, the only supported slot for shelves.

Option 1: Cable to 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.



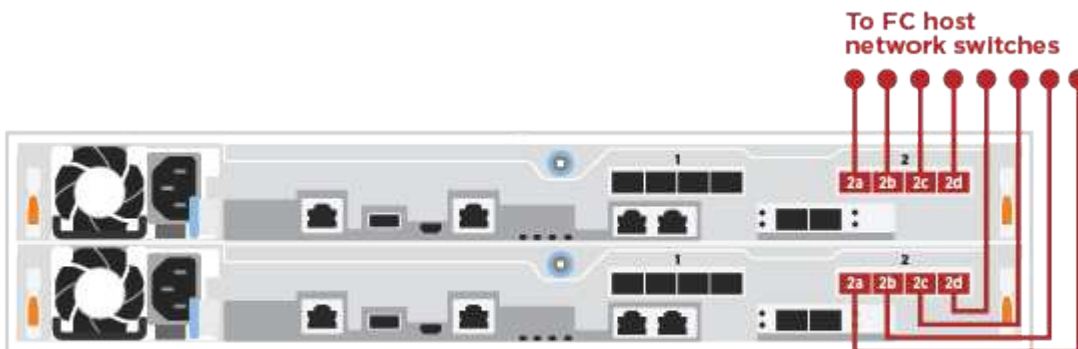
As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again..

About this task

Perform the following step on each controller module.

Steps

1. Cable ports 2a through 2d to the FC host switches.

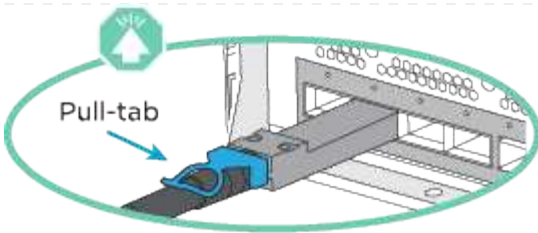


Option 2: Cable to 25GbE data or host network

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.



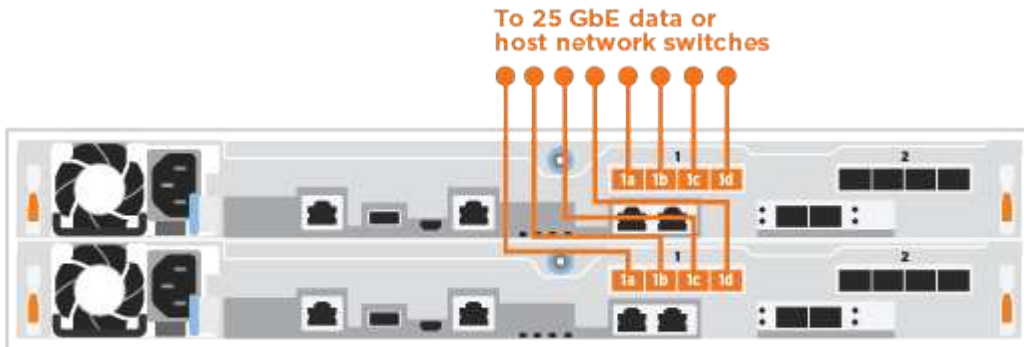
As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

About this task

Perform the following step on each controller module.

Steps

1. Cable ports e4a through e4d to the 10GbE host network switches.

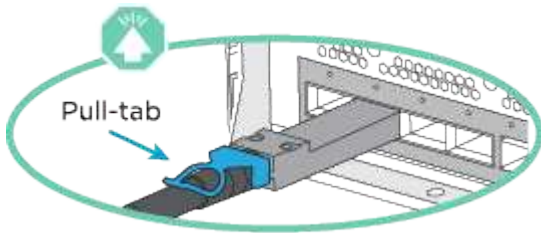


Option 3: Cable controllers to single drive shelf

Cable each controller to the NSM modules on the NS224 drive shelf.

Before you begin

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.

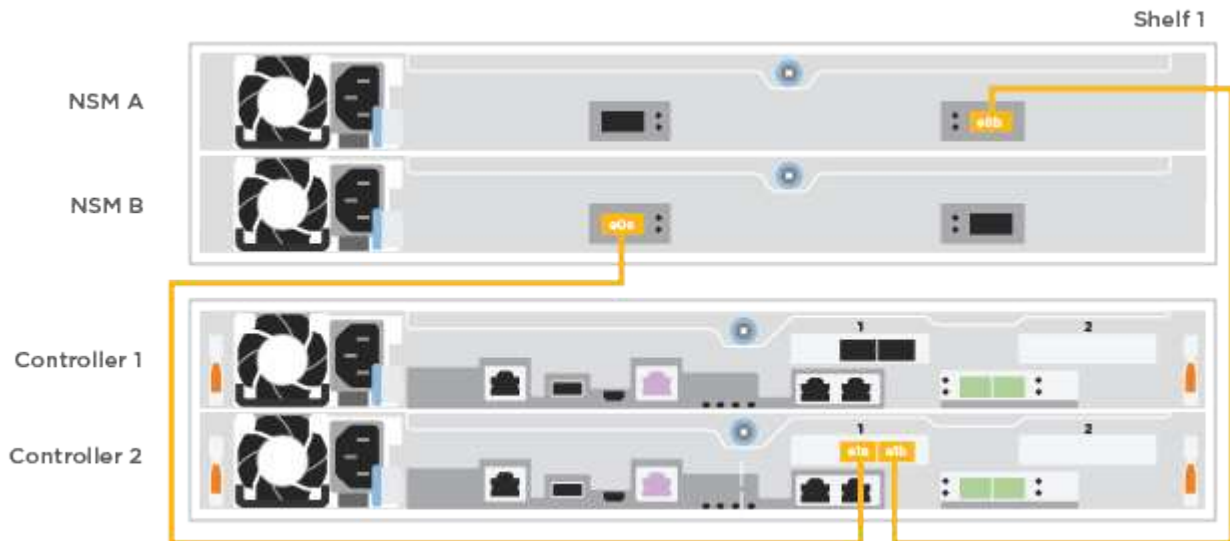
About this task

Use the animation or the tabulated steps to complete the cabling between the controllers and the single shelf. Perform the steps on each controller module.

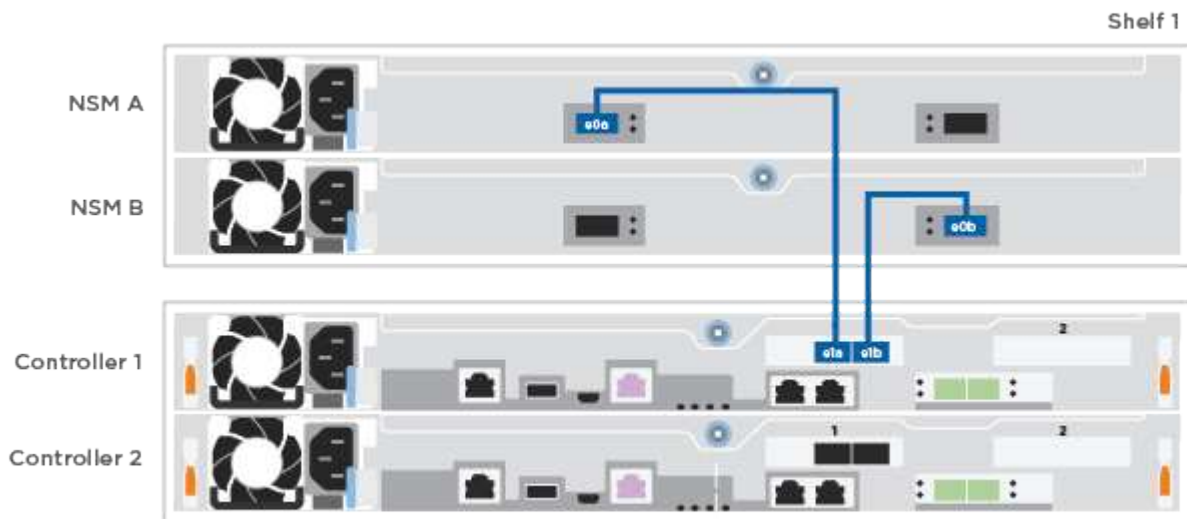
Animation - Cable the controllers to a single NS224

Steps

1. Cable controller A to the shelf.



2. Cable controller B to the shelf.



Step 5: Complete system setup

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.

Steps

1. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.

The system begins to boot. Initial booting may take up to eight minutes.

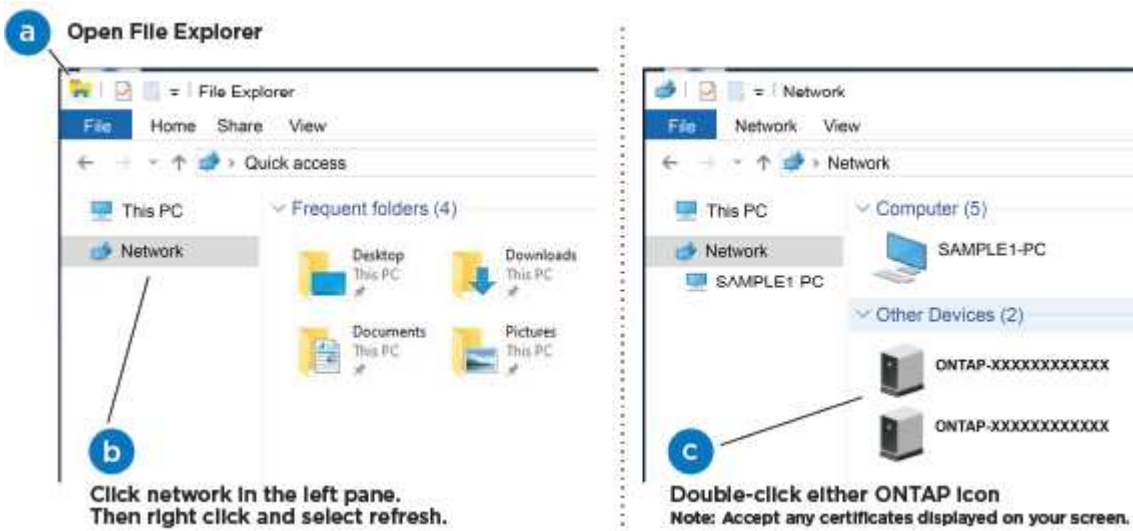
2. Make sure that your laptop has network discovery enabled.

See your laptop's online help for more information.

3. Use the animation to connect your laptop to the Management switch:

[Animation - 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 and right-click and select **refresh**.
- c. 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 [ONTAP 9 documentation](#) for information about configuring additional features in ONTAP.

Option 2: 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.

The system begins to boot. Initial booting may take up to eight minutes.

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	<ol style="list-style-type: none">a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. <div> Check your laptop or console's online help if you do not know how to configure PuTTY.</div> <ol style="list-style-type: none">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 [ONTAP 9 documentation](#) for information about configuring additional features in ONTAP.

Maintain

Maintain ASA C250 hardware

For the ASA C250 storage system, you can perform maintenance procedures on the following components.

Boot media

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

Chassis

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

Controller

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

DIMM

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

Drive

A drive is a device that provides the physical storage media for data.

Fan

The fan cools the controller.

Mezzanine card

A Mezzanine card is a printed circuit board that plugs directly into another plug-in card.

NVEM battery

A battery is included with the controller and preserves cached data if the AC power fails.

Power supply

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

Real-time clock battery

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

Boot media

Overview of boot media replacement - ASA C250

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

Before you begin

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

About this task

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

Check encryption key support and status - ASA C250

To ensure data security on your storage system, you need to verify the encryption key support and status on your boot media. Check if your ONTAP version supports NetApp Volume Encryption (NVE), and before you shut down the controller check if the key manager is active.

Step 1: Check if your version of ONTAP supports NetApp Volume Encryption

Check whether your ONTAP version supports NetApp Volume Encryption (NVE). This information is crucial for downloading the correct ONTAP image.

Steps

1. Determine if your ONTAP version supports encryption by running the following command:

```
version -v
```

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

2. Depending on whether NVE is supported on your system, take one of the following actions:
 - If NVE is supported, download the ONTAP image with NetApp Volume Encryption.
 - If NVE is not supported, download the ONTAP image **without** NetApp Volume Encryption.

Step 2: Determine if it is safe to shut down the controller

To safely shut down a controller, first identify whether the External Key Manager (EKM) or the Onboard Key Manager (OKM) is active. Then, verify the key manager in use, display the appropriate key information, and take action based on the status of the authentication keys.

Steps

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

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

2. Depending on whether a key manger is configured on your system, select one of the following options.

No key manager configured

You can safely shut down the impaired controller. Go to [shutdown the impaired controller](#).

External or Onboard key manager configured

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

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

- b. Check the output for the value in the `Restored` column for your key manager.

This column indicates whether the authentication keys for your key manager (either EKM or OKM) have been successfully restored.

3. Depending on whether your system is using the External Key Manager or Onboard Key Manager, select one of the following options.

External Key Manager

Depending on the output value displayed in the `Restored` column, follow the appropriate steps.

Output value in <code>Restored</code> column	Follow these steps...
true	You can safely shut down the impaired controller. Go to shutdown the impaired controller .
Anything other than true	<p>a. Restore the external key management authentication keys to all nodes in the cluster using the following command:</p> <pre>security key-manager external restore</pre> <p>If the command fails, contact NetApp Support.</p> <p>b. Verify that the <code>Restored</code> column displays true for all authentication keys by entering the <code>security key-manager key query</code> command.</p> <p>If all the authentication keys are true, you can safely shut down the impaired controller. Go to shutdown the impaired controller.</p>

Onboard Key Manager

Depending on the output value displayed in the `Restored` column, follow the appropriate steps.

Output value in <code>Restored</code> column	Follow these steps...
true	<p>Manually back up the OKM information.</p> <p>a. Go to the advanced mode by entering <code>set -priv advanced</code> and then enter <code>Y</code> when prompted.</p> <p>b. Enter the following command to display the key management information:</p> <pre>security key-manager onboard show-backup</pre> <p>c. Copy the contents of the backup information to a separate file or your log file.</p> <p>You'll need it in disaster scenarios where you might need to manually recover OKM.</p> <p>d. You can safely shut down the impaired controller. Go to shutdown the impaired controller.</p>

Output value in Restored column	Follow these steps...
Anything other than true	<p>a. Enter the onboard security key-manager sync command:</p> <pre>security key-manager onboard sync</pre> <p>b. Enter the 32 character, alphanumeric onboard key management passphrase when prompted.</p> <p>If the passphrase cannot be provided, contact NetApp Support.</p> <p>c. Verify the Restored column displays true for all authentication keys:</p> <pre>security key-manager key query</pre> <p>d. Verify that the Key Manager type displays onboard, and then manually back up the OKM information.</p> <p>e. Enter the command to display the key management backup information:</p> <pre>security key-manager onboard show-backup</pre> <p>f. Copy the contents of the backup information to a separate file or your log file.</p> <p>You'll need it in disaster scenarios where you might need to manually recover OKM.</p> <p>g. You can safely shut down the impaired controller. Go to shutdown the impaired controller.</p>

Shut down the controller - ASA C250

Option 1: Most systems

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

Steps

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

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



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

Option 2: Systems 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 [Synchronize a node with the cluster](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

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

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

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

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

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

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

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

Replace the boot media - ASA C250

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

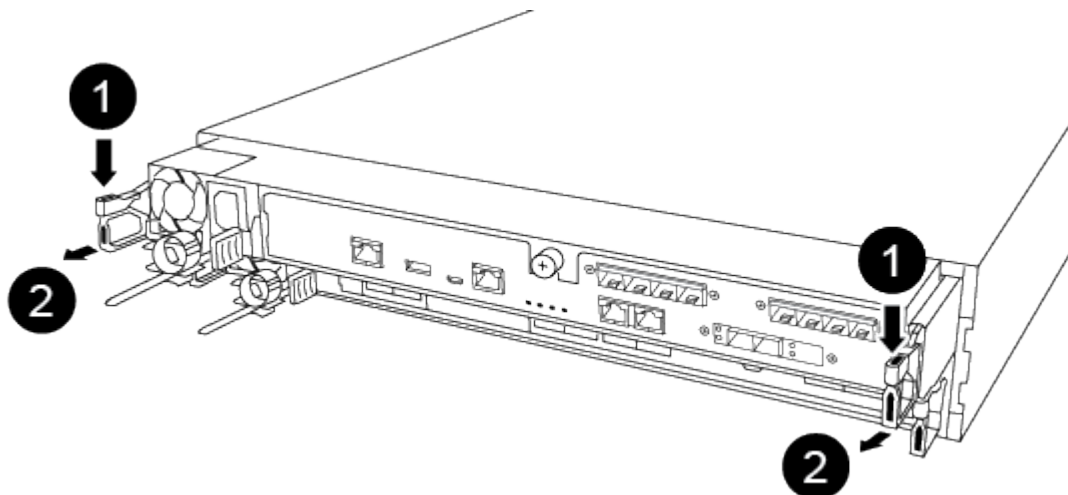
To access components inside the controller module, you must first remove the controller module from the system, and then remove the cover on the controller module.

Steps

1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.
4. Unplug the I/O cables from the controller module.
5. 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.

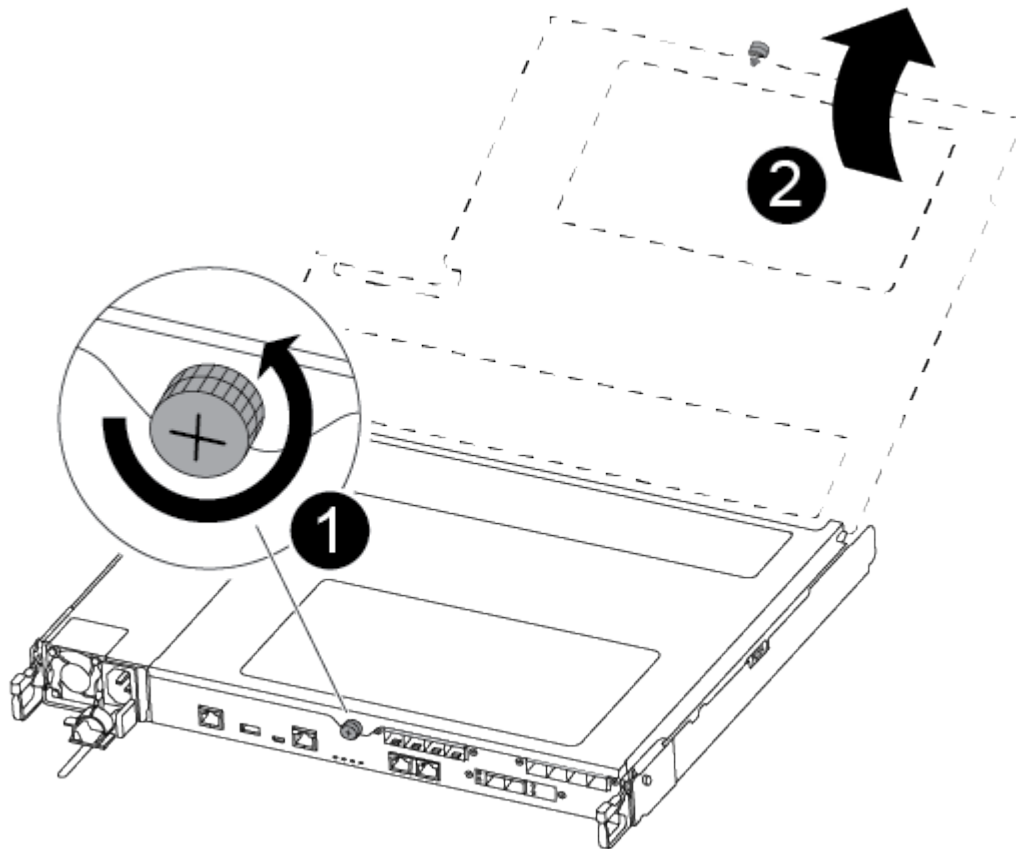


If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



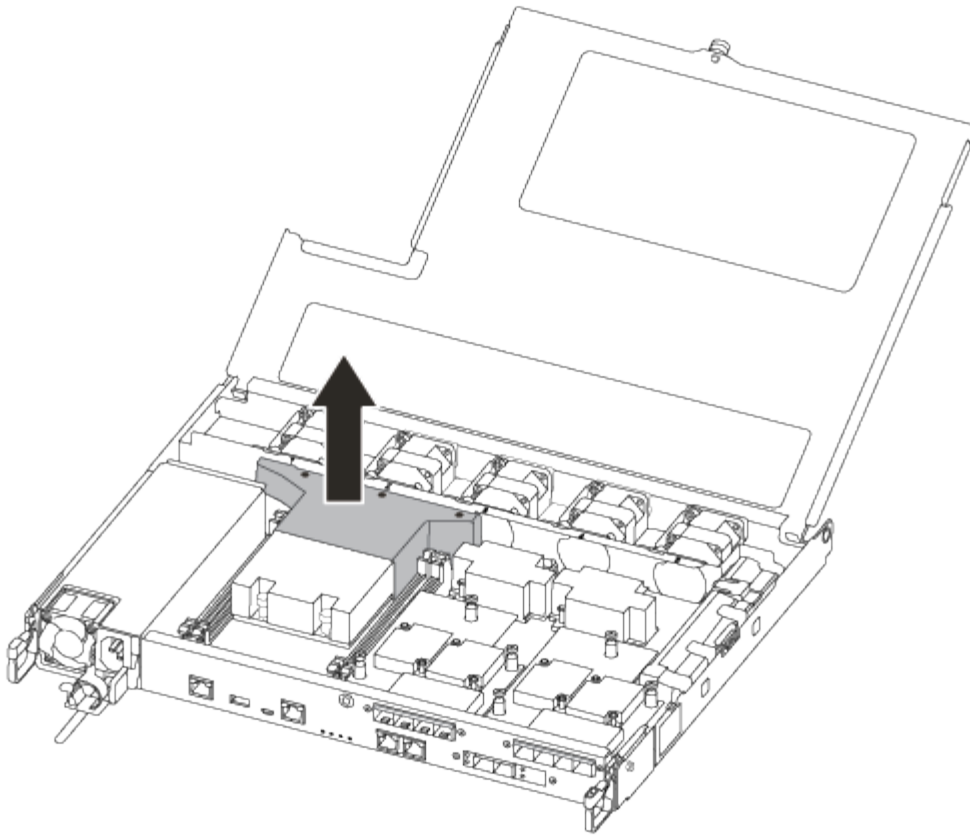
1	Lever
2	Latching mechanism

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



1	Thumbscrew
2	Controller module cover.

8. Lift out the air duct cover.



Step 2: Replace the boot media

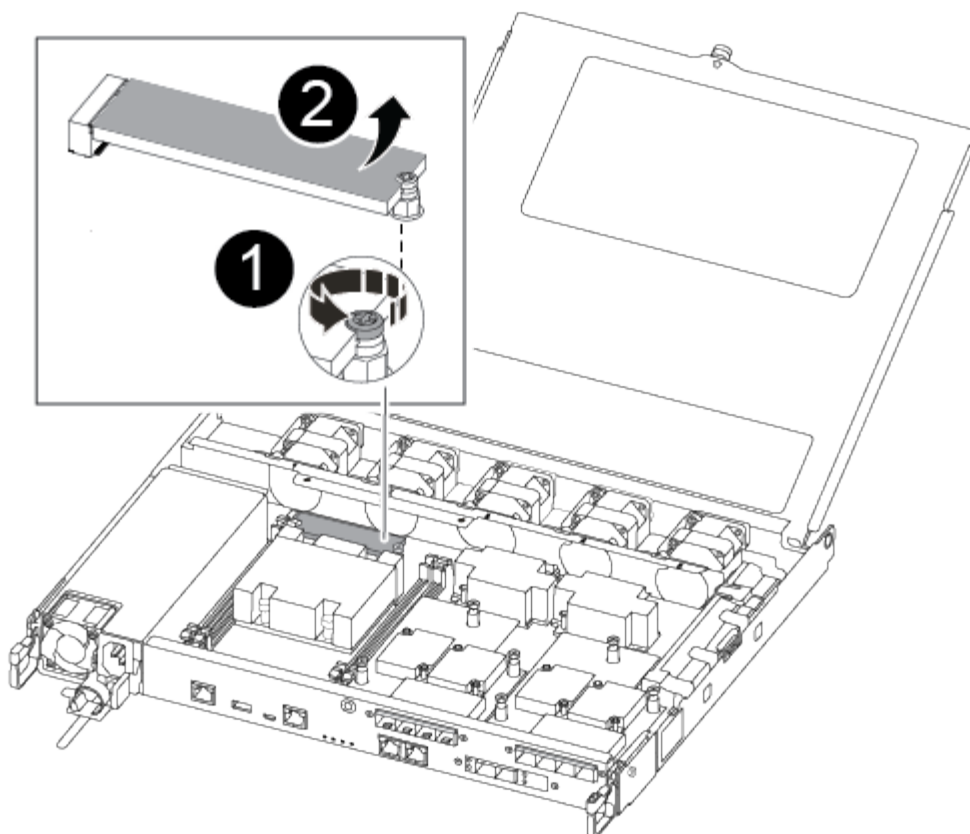
You locate the failed boot media in the controller module by removing the air duct on the controller module before you can replace the boot media.

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 lose it.

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

[Animation - Replace 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.

2. Using the #1 magnetic screwdriver, remove the screw from the impaired boot media, and set it aside safely on the magnet.
3. Gently lift the impaired boot media directly out of the socket and set it aside.
4. Remove the replacement boot media from the antistatic shipping bag and align it into place on the controller module.
5. 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.
 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

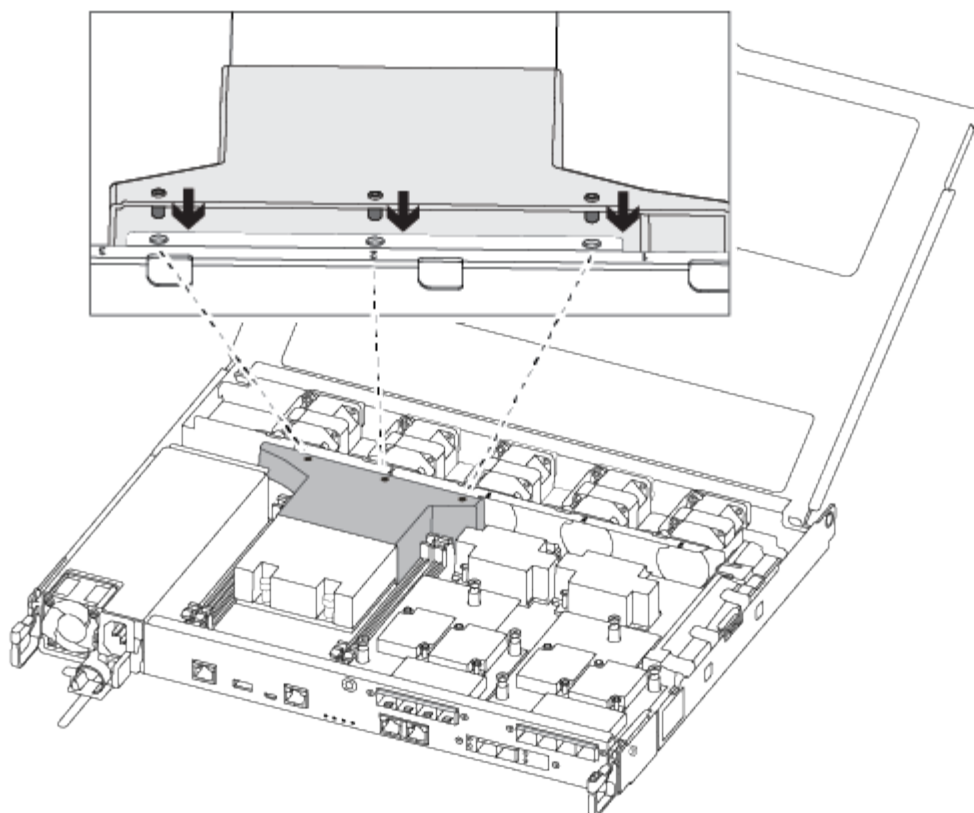
4. Copy the efi folder to the top directory on the USB flash drive.



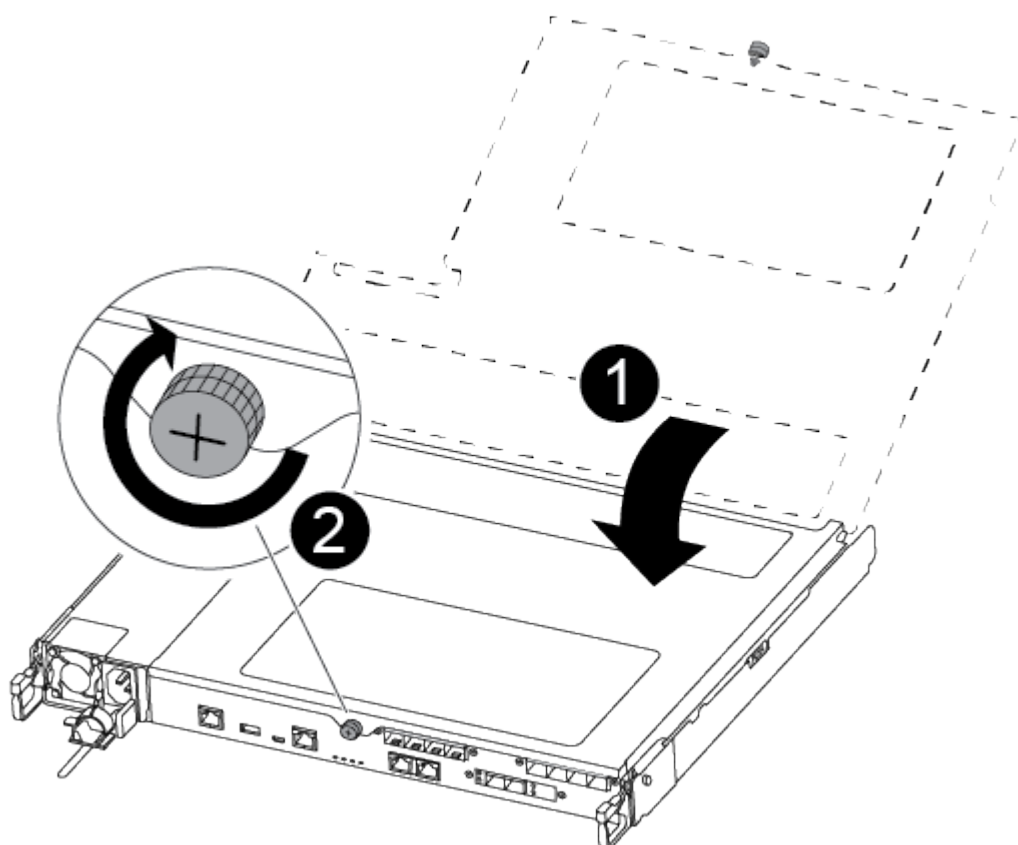
If the service image has no efi folder, see [EFI folder missing from Service Image download file used for boot device recovery for FAS and AFF models^](#) .

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.



1	Controller module cover
2	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. 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.

10. Push the controller module all the way into the chassis:

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

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

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

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

14. Reconnect the controller module I/O cables.

15. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

16. 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.

17. 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.

Boot the recovery image - ASA C250

After installing the new boot media device in your system, you can boot the recovery image from a USB drive and restore the configuration from the partner node.

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:

Option 1: ONTAP 9.16.0 or earlier

- a. On the impaired controller, press `Y` when you see `Do you want to restore the backup configuration now?`
- b. If prompted on the impaired controller, press `Y` to overwrite `/etc/ssh/ssh_host_ecdsa_key`.
- c. On the healthy partner controller, set the impaired controller to advanced privilege level: `set -privilege advanced`.
- d. On the healthy partner controller, run the restore backup command: `system node restore-backup -node local -target-address impaired_node_IP_address`.

NOTE: If you see any message other than a successful restore, contact [NetApp Support](#).

- e. On the healthy partner controller, return the impaired controller to admin level: `set -privilege admin`.
- f. On the impaired controller, press `Y` when you see `Was the restore backup procedure successful?`.
- g. On the impaired controller, press `Y` when you see `...would you like to use this restored copy now?`.
- h. On the impaired controller, press `Y` when prompted to reboot the impaired controller and press `ctrl-c` for the Boot Menu.
- i. If the system does not use encryption, select *Option 1 Normal Boot.*, otherwise go to [Restore encryption](#).

Option 2: ONTAP 9.16.1 or later

- a. On the impaired controller, press `Y` when prompted to restore the backup configuration.

After restore procedure is successful, this message will be seen on the console -
`syncflash_partner: Restore from partner complete.`

- b. On the impaired controller, press `Y` when prompted to confirm if the restore backup was successful.
- c. On the impaired controller, press `Y` when prompted to use the restored configuration.
- d. On the impaired controller, press `Y` when prompted to reboot the node.
- e. On the impaired controller, press `Y` when prompted to reboot the impaired controller and press `ctrl-c` for the Boot Menu.
- f. If the system does not use encryption, select *Option 1 Normal Boot.*, otherwise go to [Restore encryption](#).

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

7. If AutoSupport is enabled, restore/unsuppress automatic case creation by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.

NOTE: If the process fails, contact [NetApp Support](#).

Restore encryption - ASA C250

Restore encryption on the replacement boot media.

You must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled using the settings that you captured at the beginning of the boot media replace procedure.

Depending on which a key manger is configured on your system, select one of the following options to restore it from the boot menu.

- [Option 1: Restore the Onboard Key Manager configuration](#)
- [Option 2: Restore the External Key Manager configuration](#)

Option 1: Restore the Onboard Key Manager configuration

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

Before you begin

- Make sure you have following information while restoring the OKM configuration:
 - Cluster-wide passphrase entered [while enabling onboard key management](#).
 - [Backup information for the Onboard Key Manager](#).
- Perform the [How to verify onboard key management backup and cluster-wide passphrase](#) procedure before proceeding.

Steps

1. Connect the console cable to the target controller.
2. From the ONTAP boot menu select the appropriate option from the boot menu.

ONTAP version	Select this option
ONTAP 9.8 or later	<p data-bbox="621 153 833 191">Select option 10.</p> <p data-bbox="621 222 951 260">Show example boot menu</p> <div data-bbox="654 296 1456 1081"> <p data-bbox="683 333 1294 367">Please choose one of the following:</p> <ul data-bbox="683 411 1369 1010" style="list-style-type: none"> <li data-bbox="683 411 971 445">(1) Normal Boot. <li data-bbox="683 453 1133 487">(2) Boot without /etc/rc. <li data-bbox="683 495 1045 529">(3) Change password. <li data-bbox="683 537 1369 604">(4) Clean configuration and initialize all disks. <li data-bbox="683 613 1154 646">(5) Maintenance mode boot. <li data-bbox="683 655 1328 688">(6) Update flash from backup config. <li data-bbox="683 697 1240 730">(7) Install new software first. <li data-bbox="683 739 971 772">(8) Reboot node. <li data-bbox="683 781 1192 848">(9) Configure Advanced Drive Partitioning. <li data-bbox="683 856 1333 924">(10) Set Onboard Key Manager recovery secrets. <li data-bbox="683 932 1317 999">(11) Configure node for external key management. <p data-bbox="683 1016 1032 1050">Selection (1-11)? 10</p> </div>

ONTAP version	Select this option
ONTAP 9.7 and earlier	<p>Select the hidden option <code>recover_onboard_keymanager</code></p> <p>Show example boot menu</p> <div> <pre> Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager </pre> </div>

3. Confirm that you want to continue the recovery process.

Show example prompt

```

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

```

4. Enter the cluster-wide passphrase twice.

While entering the passphrase the console will not show any input.

Show example prompt

```

Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:

```

5. Enter the backup information.

a. Paste the entire content from the BEGIN BACKUP line through the END BACKUP line.

Show example prompt

Enter the backup data:

```
-----BEGIN BACKUP-----
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----
```

b. Press the enter key twice at the end of the input.

The recovery process completes.

Show example prompt

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

Successfully recovered keymanager secrets.

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



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

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

Show example prompt

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

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

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

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

8. From the partner node, giveback the partner controller by entering the following command.

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

9. After booting with only the CFO aggregate, run the following command.

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

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

Show example prompt

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

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



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

11. Ensure that all keys are synced by entering the following command.

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

There are no entries matching your query.



No results should appear when filtering for false in the restored parameter.

12. Giveback the node from the partner by entering the following command.

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

13. Restore automatic giveback, if you disabled it, by entering the following command.

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

14. If AutoSupport is enabled, restore automatic case creation by entering the following command.

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

Option 2: Restore the External Key Manager configuration

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

Before you begin

You need the following information for restoring the External Key Manager (EKM) configuration.

- A copy of the /cfcard/kmip/servers.cfg file from another cluster node or the following information:
 - The KMIP server address.
 - The KMIP port.
- A copy of the /cfcard/kmip/certs/client.crt file from another cluster node or the client certificate.

- A copy of the `/cfcard/kmip/certs/client.key` file from another cluster node or the client key.
- A copy of the `/cfcard/kmip/certs/CA.pem` file from another cluster node or the KMIP server CA(s).

Steps

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

Show example boot menu

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

3. When prompted, confirm you have gathered the required information.

Show example prompt

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

4. When prompted, enter the client and server information.

Show prompt

```
Enter the client certificate (client.crt) file contents:
Enter the client key (client.key) file contents:
Enter the KMIP server CA(s) (CA.pem) file contents:
Enter the server configuration (servers.cfg) file contents:
```

Show example

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

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

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

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

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

After you enter the client and server information, the recovery process completes.

Show example

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

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

Show example prompt

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

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

6. Restore automatic giveback if you disabled it.

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

7. If AutoSupport is enabled, restore automatic case creation by entering the following command.

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

Return the failed part to NetApp - ASA C250

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

Chassis

Overview of chassis replacement - ASA C250

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.

About this task

- 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 - ASA C250

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

Before you begin

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

Make note of any faults presently on the system, such as LEDs on the system components.

Steps

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

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

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

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

6. Exit the cluster shell:

```
exit
```

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

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

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

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



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

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

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

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

Replace hardware - ASA C250

To replace the chassis, you move the power supplies, hard drives, and controller module from the impaired chassis to the new chassis, and swap out the impaired chassis from 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.

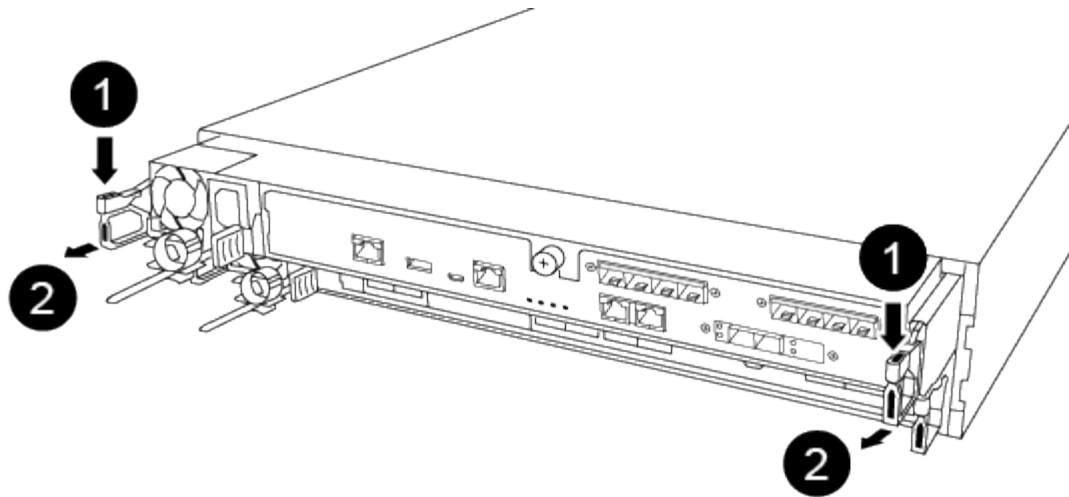
Use the following video or the tabulated steps to replace the chassis; it assumes the removal and replacement of the bezel:

[Animation - Replace 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 the 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. 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. 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 should be fully inserted and flush with the edges of the chassis.

- a. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect

the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

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

Complete the restoration and replacement process - ASA C250

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

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

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

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: Return the failed part to NetApp

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

Controller

Overview of controller module replacement- ASA C250

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 module - ASA C250

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:
 - a. Enter the following command from the console of the healthy controller:

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

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

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

Replace the controller module hardware - ASA C250

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.

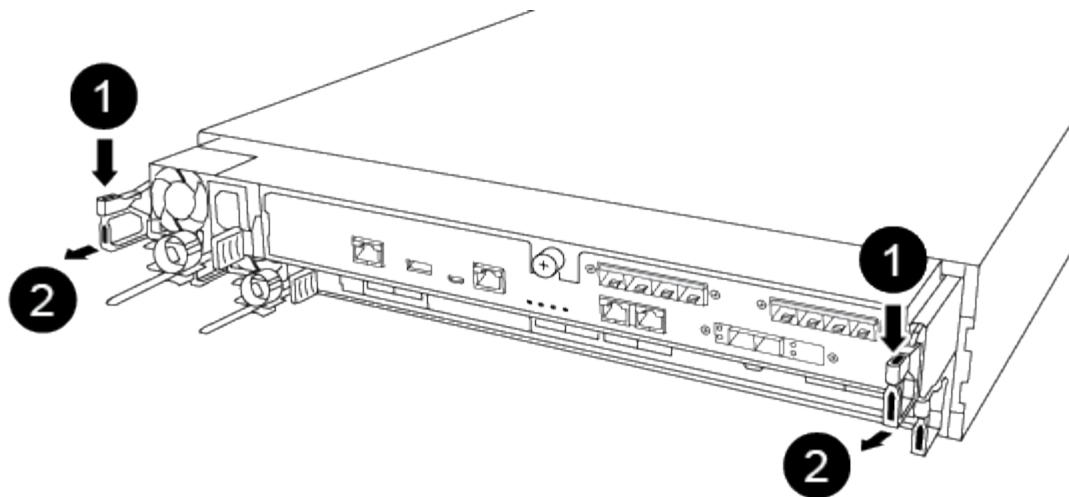
Use the following video or the tabulated steps to replace a controller module:

[Animation - Replace 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.

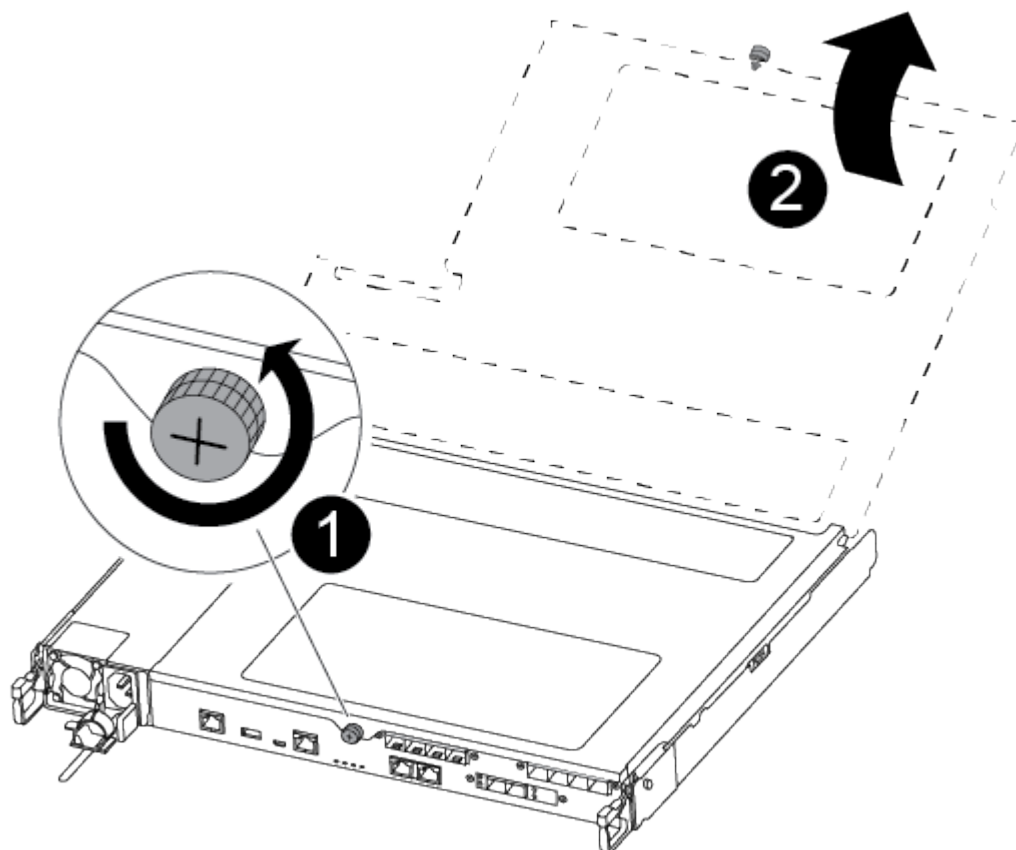


If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



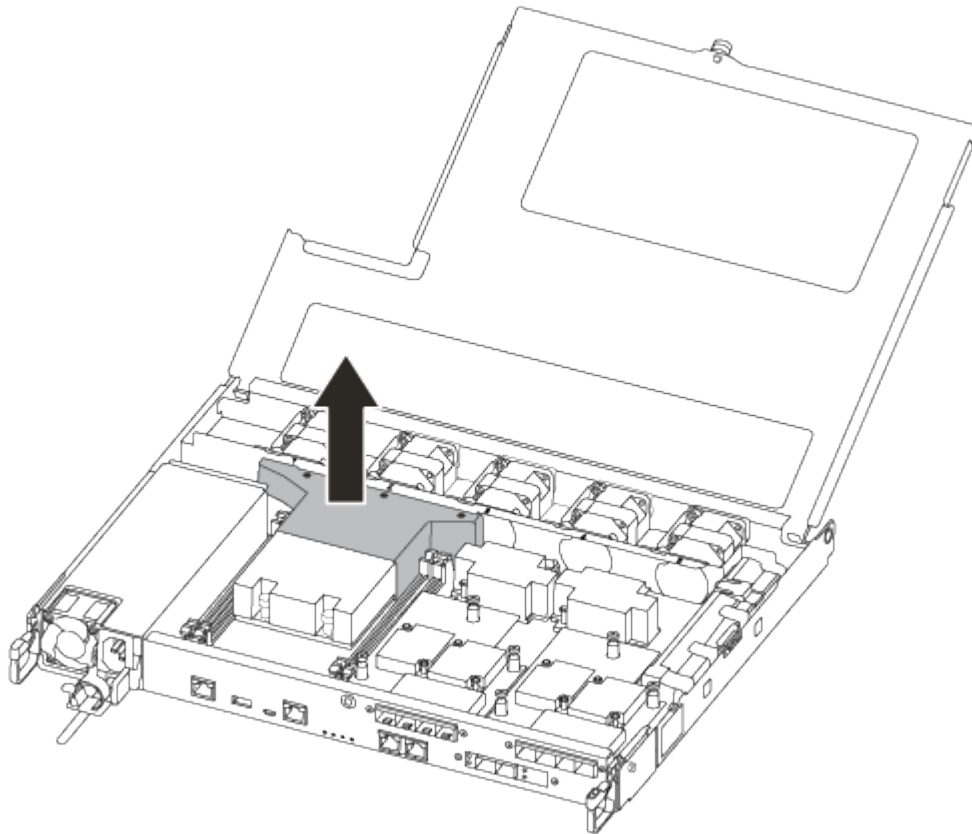
1	Lever
2	Latching mechanism

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.



1	Thumbscrew
2	Controller module cover.

7. Lift out the air duct cover.



Step 2: Move the power supply

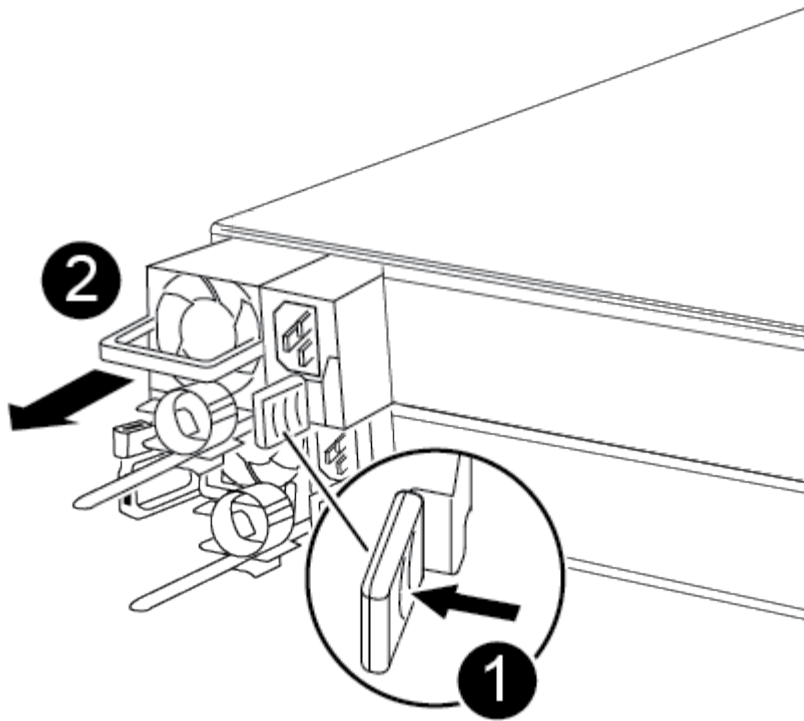
You must move the power supply from the impaired controller module to the replacement controller module when you replace a controller module.

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.

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. 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.

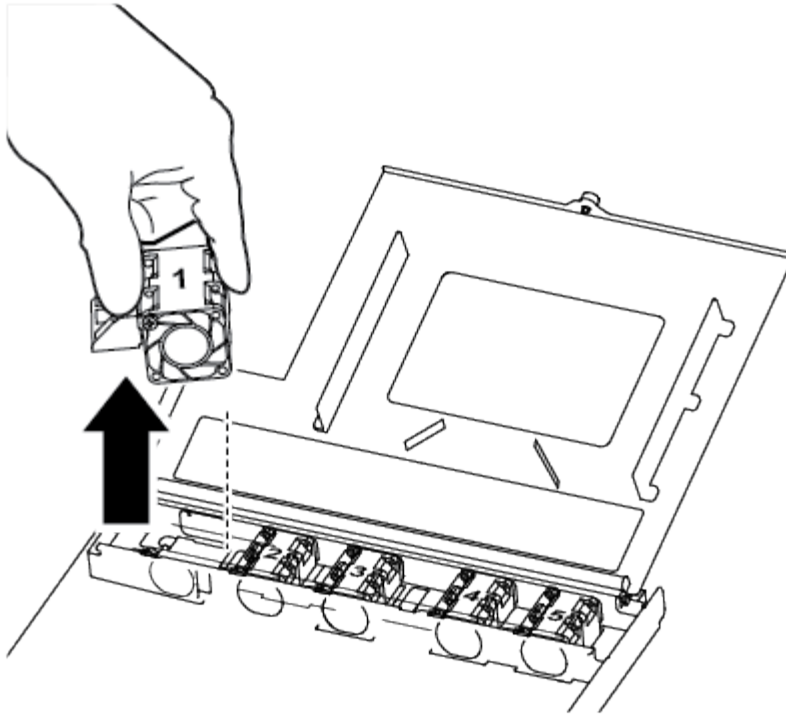


To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

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.

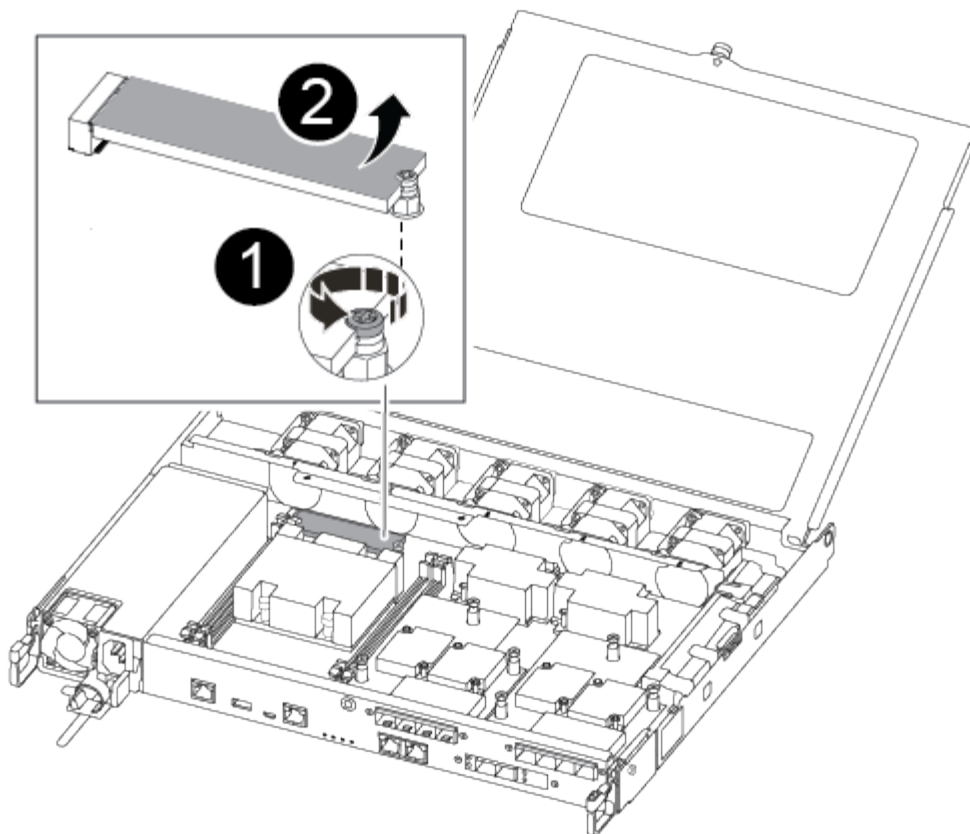
Step 4: Move the boot media

You must move the boot media device 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.

The boot media is located under the air duct cover you removed earlier in this procedure.



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.

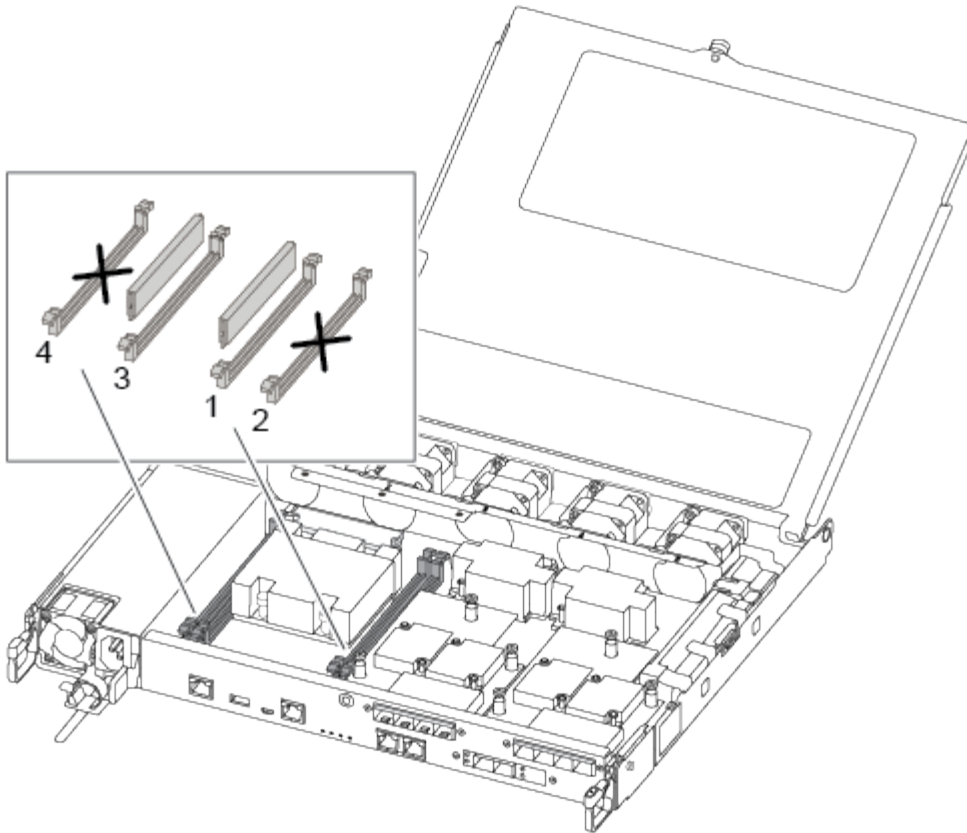
2. Using the #1 magnetic screwdriver, remove the screw from the boot media, and set it aside safely on the magnet.
3. Gently lift the boot media directly out of the socket and align it into place in the replacement controller module.
4. Using the #1 magnetic screwdriver, insert and tighten the screw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



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.

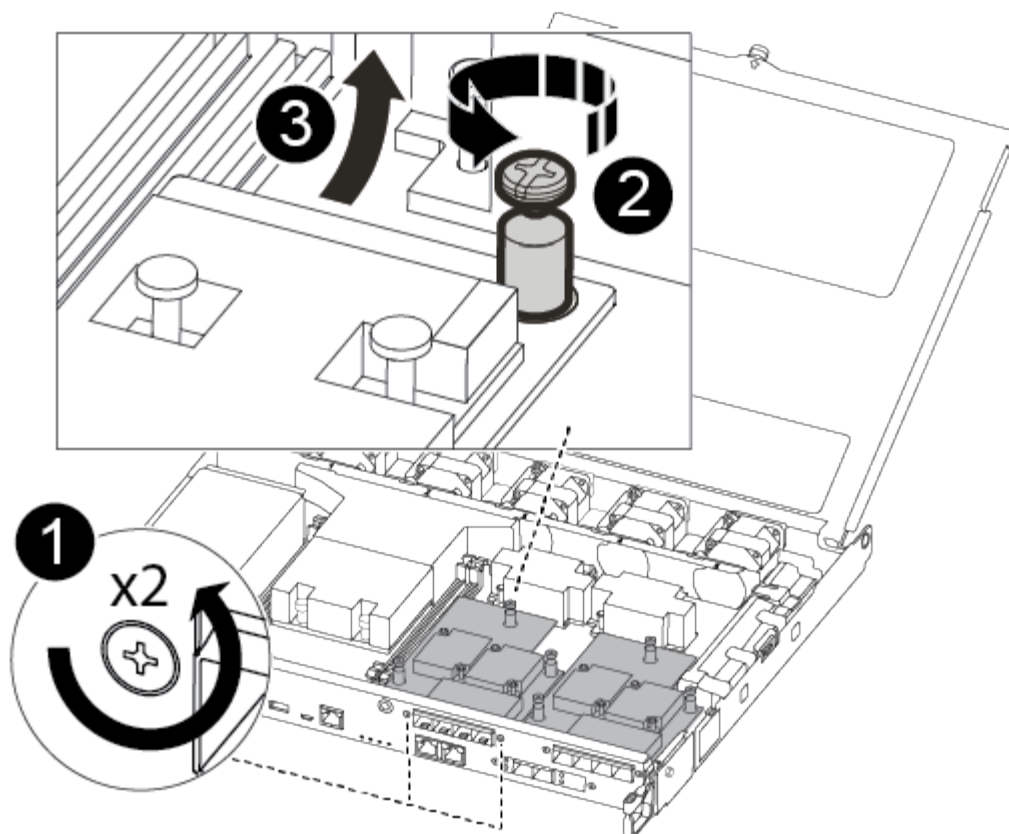
The DIMMs fit tightly in the socket. If not, reinsert the DIMM to realign it with the socket.

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.
2	Loosen the screw in the controller module.
3	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.

- Remove any SFP or QSFP modules that might be in the mezzanine card and set it aside.
- 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.
- Gently lift the mezzanine card out of the socket and move it to the same position in the replacement controller.
- Gently align the mezzanine card into place in the replacement controller.
- 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.

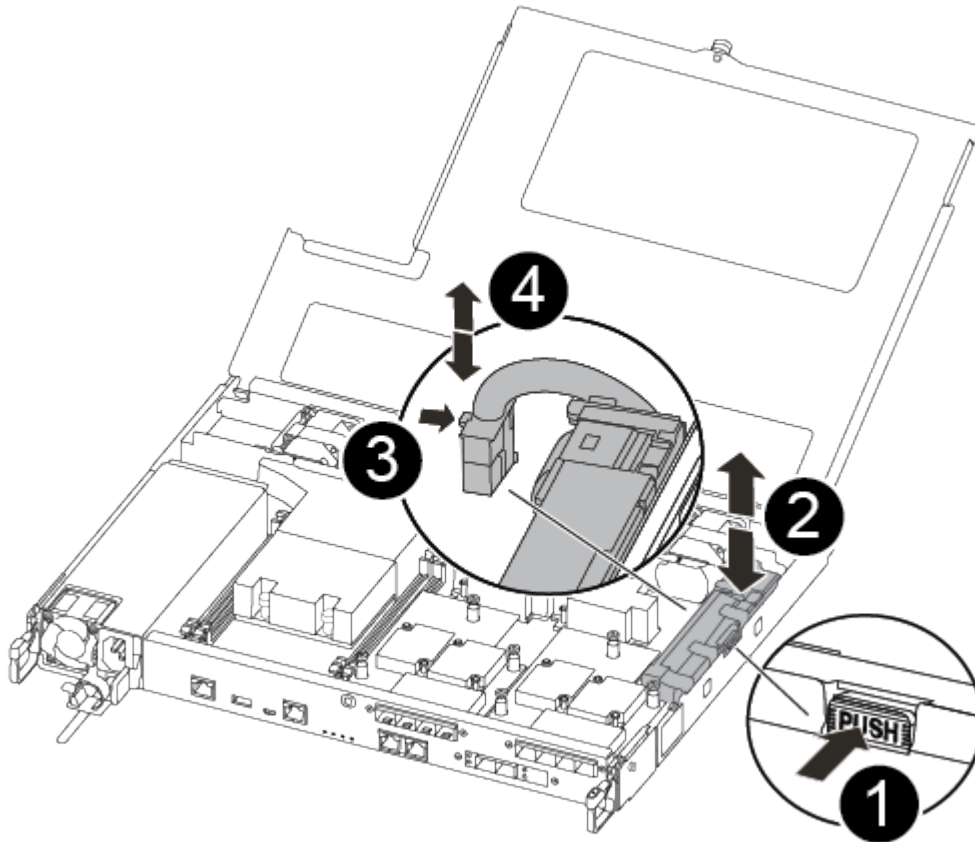
3. Repeat these steps if there is another mezzanine card in the impaired controller module.

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.

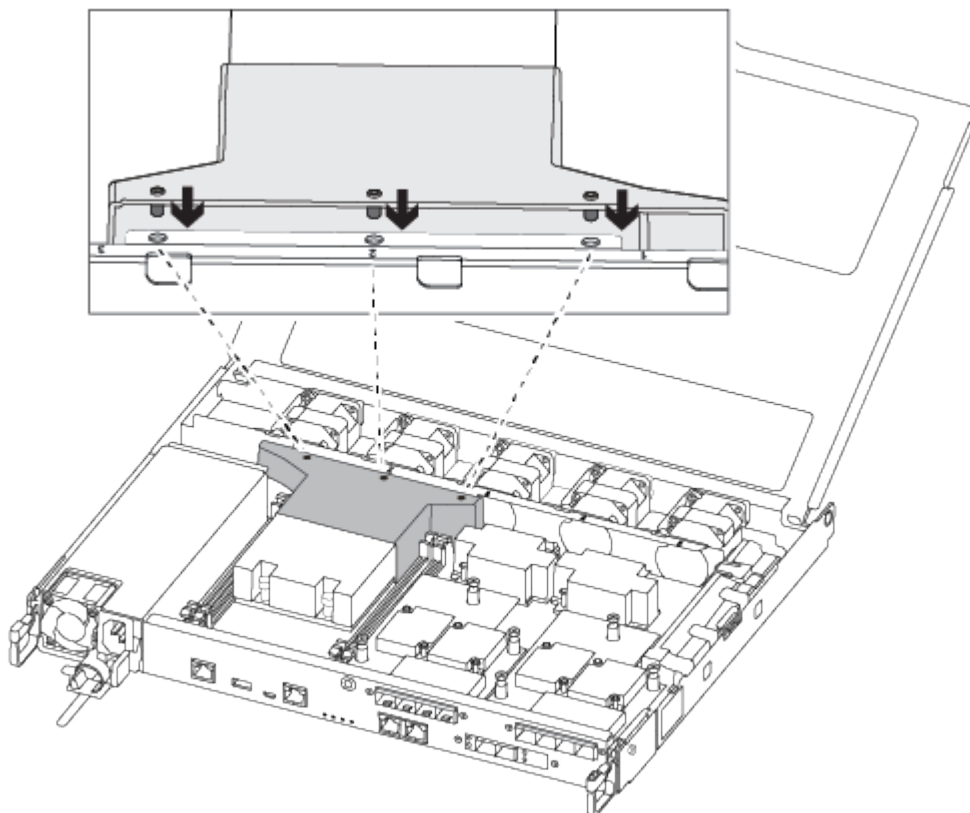
4. Locate the corresponding NV battery holder on the replacement controller module and align the NV battery to the battery holder.
5. Insert the NV battery plug into the socket.
6. Slide the battery pack down along the sheet metal side wall until the support tabs on the side wall hook into the slots 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

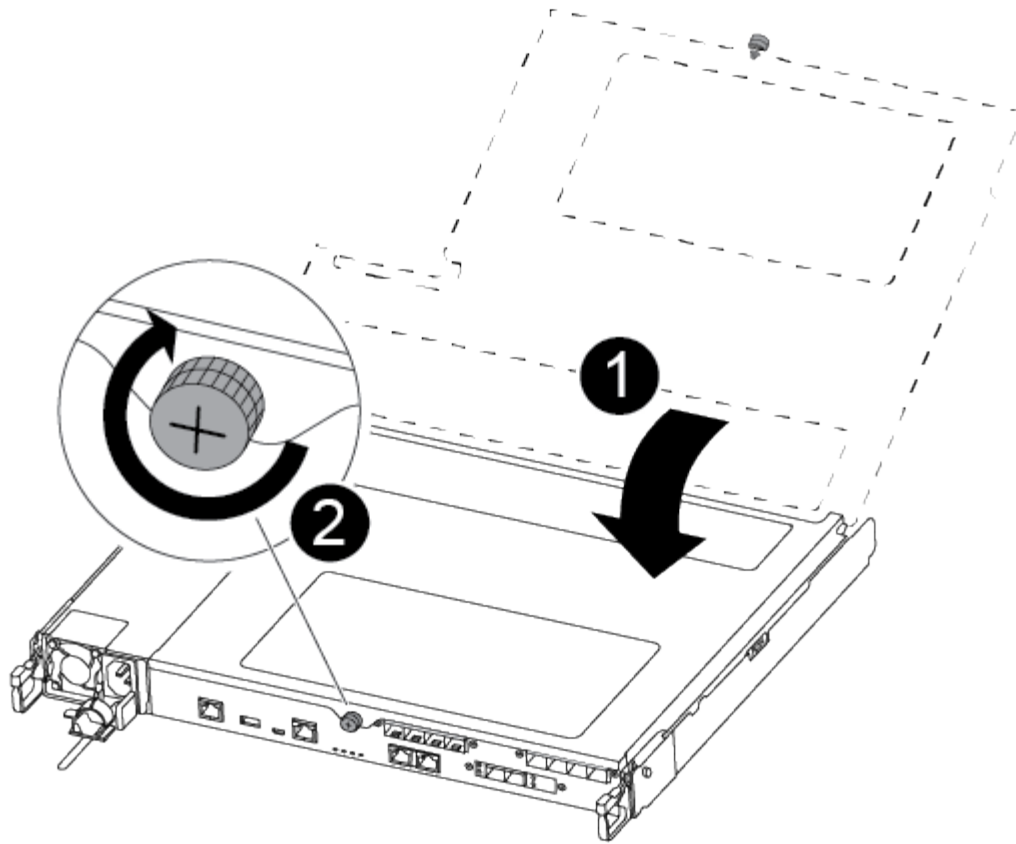
After all of the components have been moved from the impaired controller module to the replacement controller module, you must install the replacement controller module into the chassis, and then boot it to Maintenance mode.

You can use the following illustrations 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:
 - 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 should be fully inserted and flush with the edges of the chassis.

- f. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

Restore and verify the system configuration - ASA C250

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: `cluster date show`

The date and time are based on the configured timezone.

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

The date and time are given in GMT.

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

The date and time are given in GMT.

Step 2: Verify and set the HA state of the controller

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`

Recable the system and reassign disks - ASA C250

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

Step 1: Recable the system

Verify the controller module's storage and network connections.

Steps

1. 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`
```

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

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

6. Give back the 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.

- b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

The output from the `storage failover show` command should not include the System ID changed on partner message.

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

The disks belonging to the *replacement* 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
.
.
.
```

8. 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.

9. 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](#)

10. 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.

11. Verify that the expected volumes are present for each controller: `vol show -node node-name`
12. 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 - ASA C250

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.



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

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: 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 -vserver * -lif *`
2. Register the system serial number with NetApp Support.
 - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
 - If AutoSupport is not enabled, call [NetApp Support](#) to register the serial number.
3. Check the health of your cluster. See the [How to perform a cluster health check with a script in ONTAP](#) KB article for more information.
4. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.
5. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

Step 3: Return the failed part to NetApp

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

Replace a DIMM - ASA C250

You must replace a DIMM in the controller when your storage system encounters errors such as, excessive CECC (Correctable Error Correction Codes) errors that are based on Health Monitor alerts or uncorrectable ECC errors, typically caused by a single DIMM failure preventing the storage system from booting ONTAP.

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:


If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <code>-halt true</code> parameter brings you to the LOADER prompt.</p>

Step 2: Remove the controller module

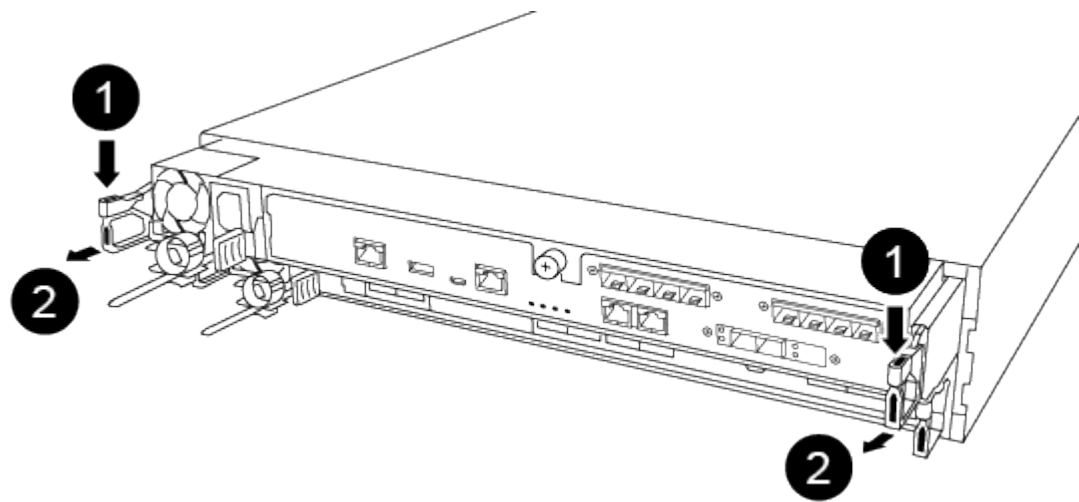
You must remove the controller module from the chassis when you replace a component inside the controller module.



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.

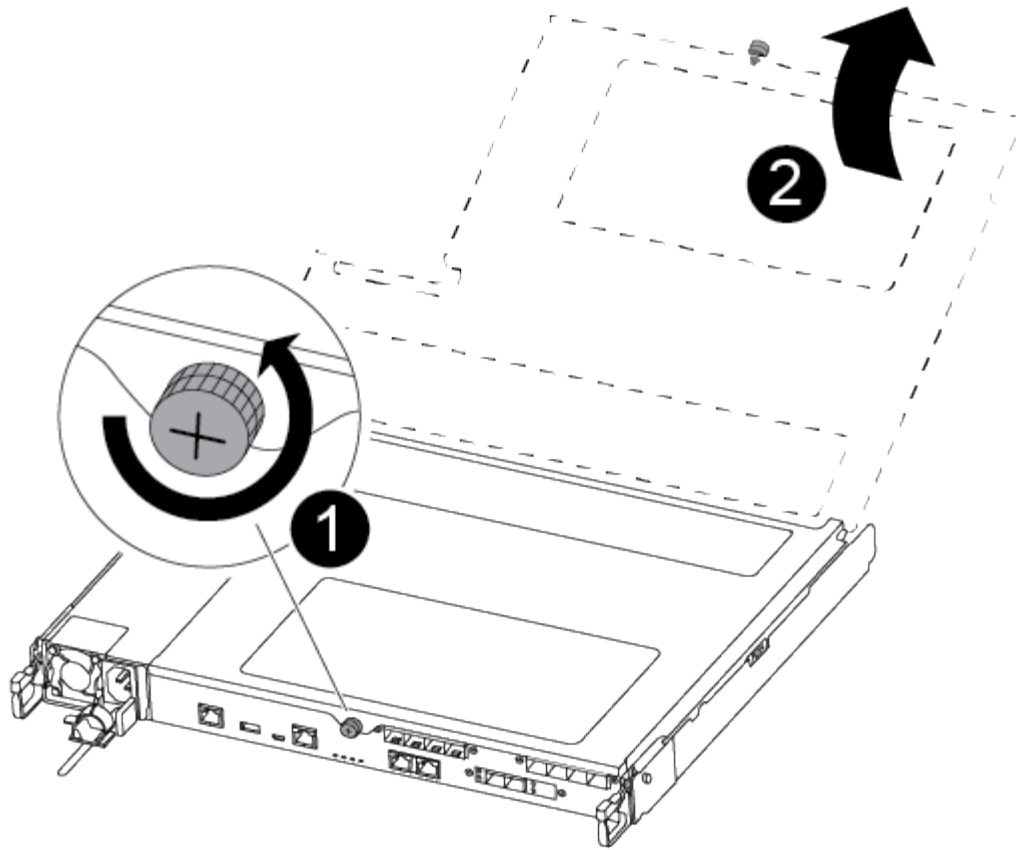


If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



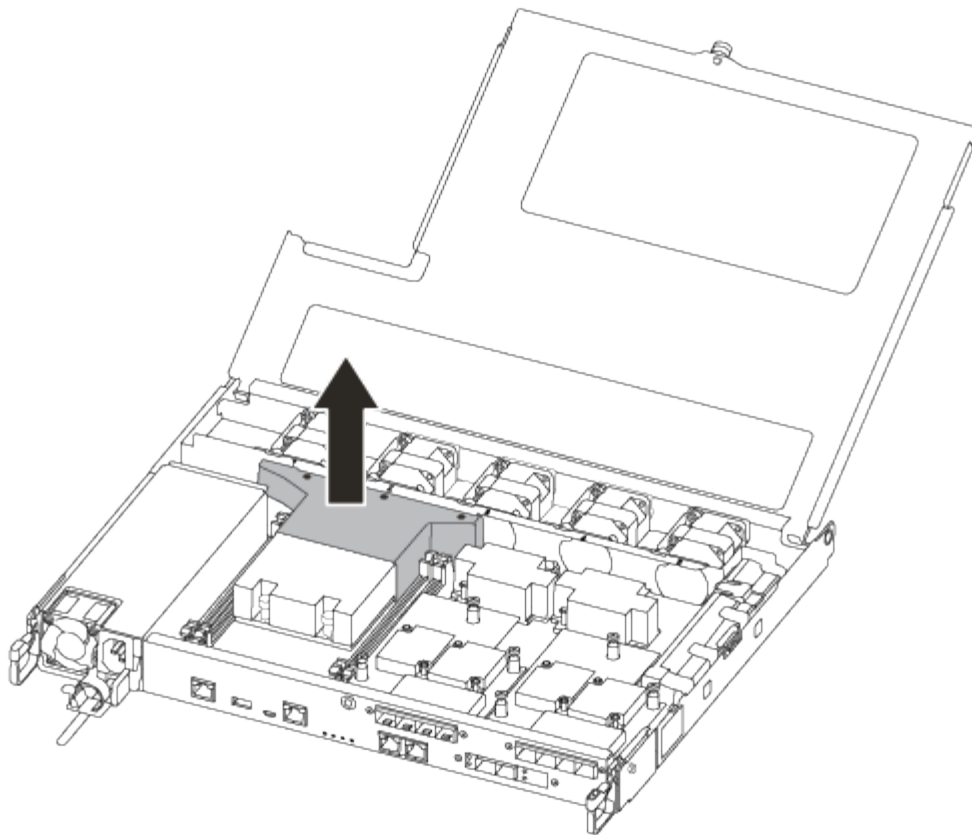
	Lever
	Latching mechanism

- 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.

7. Lift out the air duct cover.



Step 3: Replace a DIMM

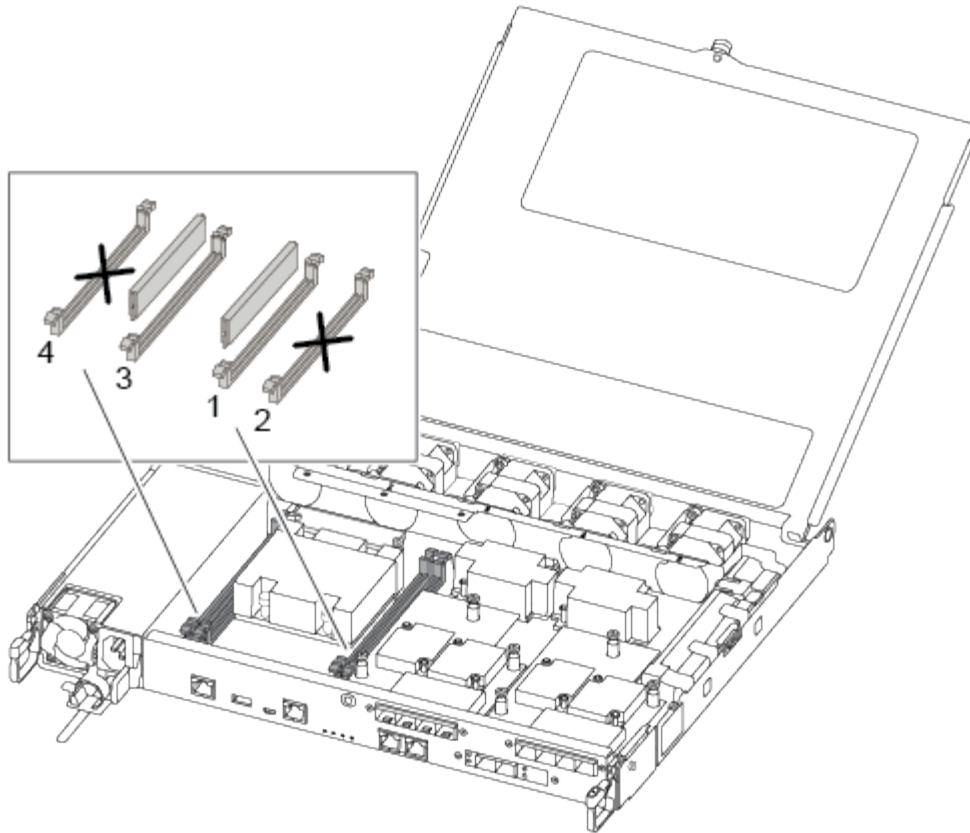
To replace a DIMM, you must locate it in the controller module using the DIMM map label on top of the air duct and then replace it following the specific sequence of steps.

Use the following video or the tabulated steps to replace a DIMM:

[Animation - Replace 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.



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.

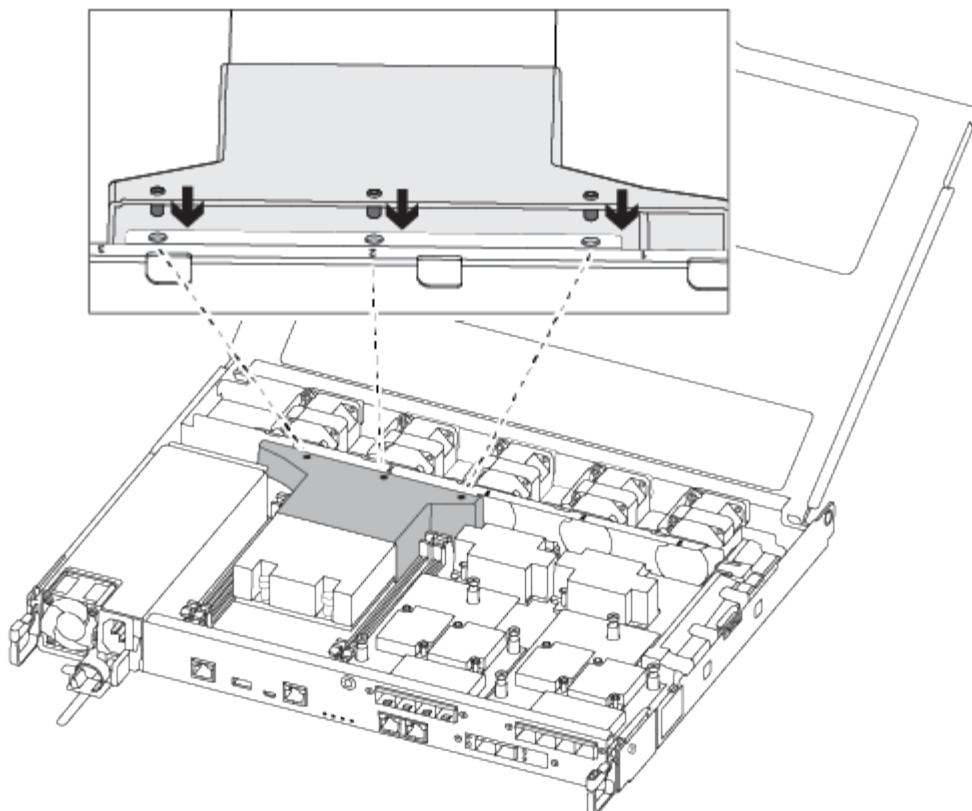
7. Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the socket.

Step 4: Install the controller module

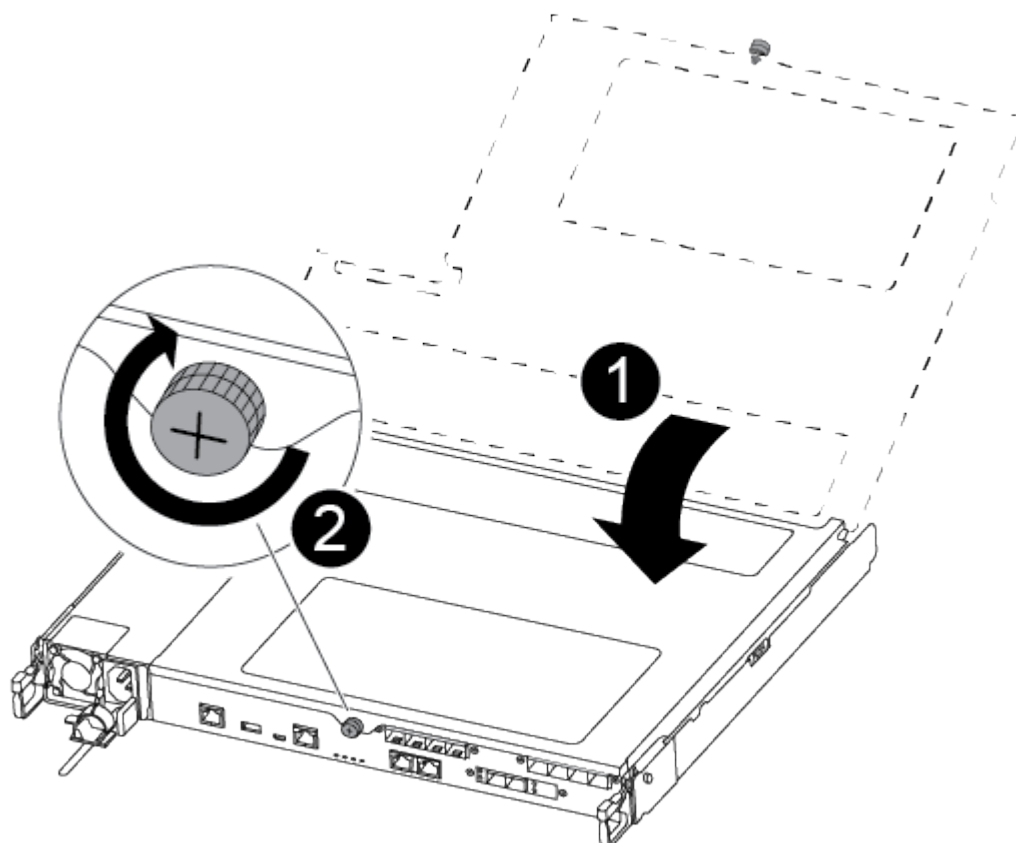
After you have replaced the component in the controller module, you must reinstall the controller module into the chassis, and then boot it.

You can use the following illustrations 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. Insert the controller module into the chassis:

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

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

4. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

5. Recable the system, as needed.

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

7. 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 and Replacements](#) page for further information.

Replace SSD Drive or HDD Drive - ASA C250

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 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 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 drive depends on how the 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 a drive, you must wait one minute between the removal of the failed drive and the insertion of the replacement drive to allow the storage system to recognize the existence of the new drive.

Option 1: Replace SSD

Steps

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

- 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 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 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 automatic 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 node_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 reenale 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 [NetApp Support](#) 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 reenale 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 automatic drive assignment in Step 1, then, manually assign drive ownership and then reenale 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 - ASA C250

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

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

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


If the impaired controller is displaying...	Then...
Waiting for giveback...	Press Ctrl-C, and then respond <i>y</i> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

Step 2: Remove the controller module

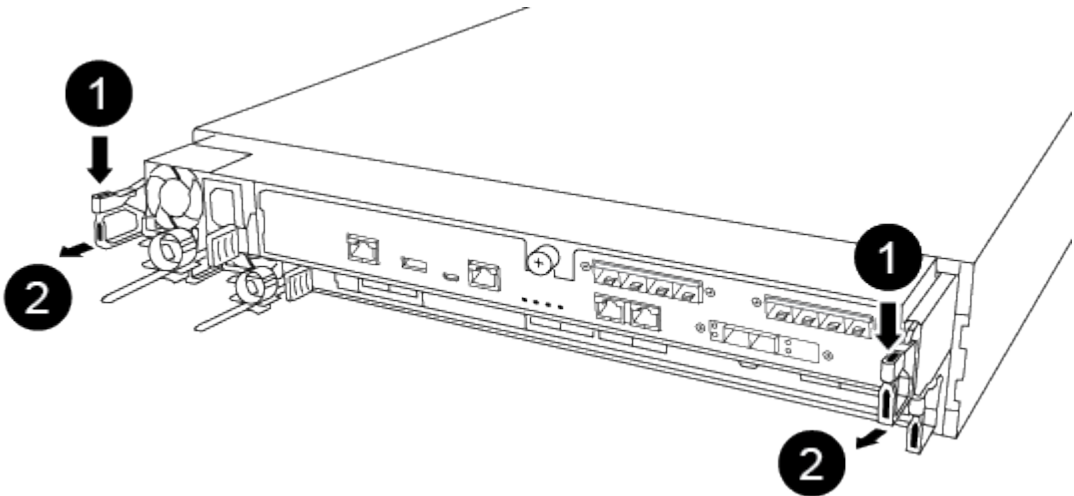
You must remove the controller module from the chassis when you replace a component inside the controller module.

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.

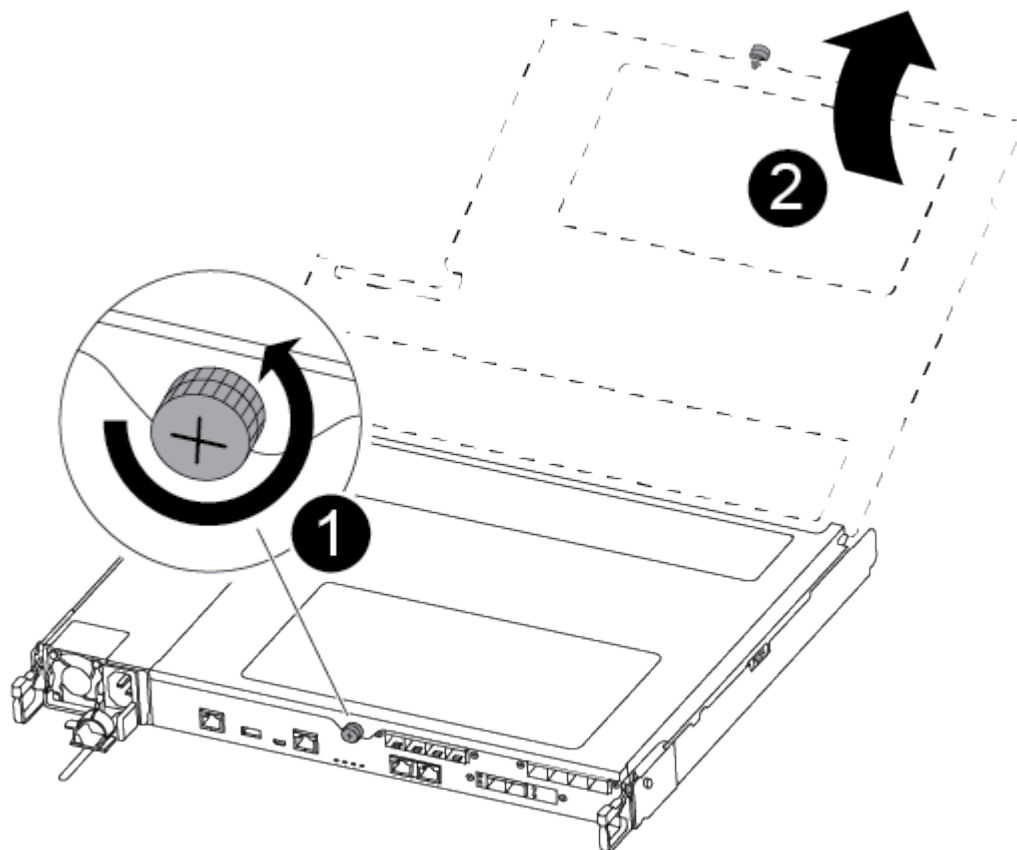


If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



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

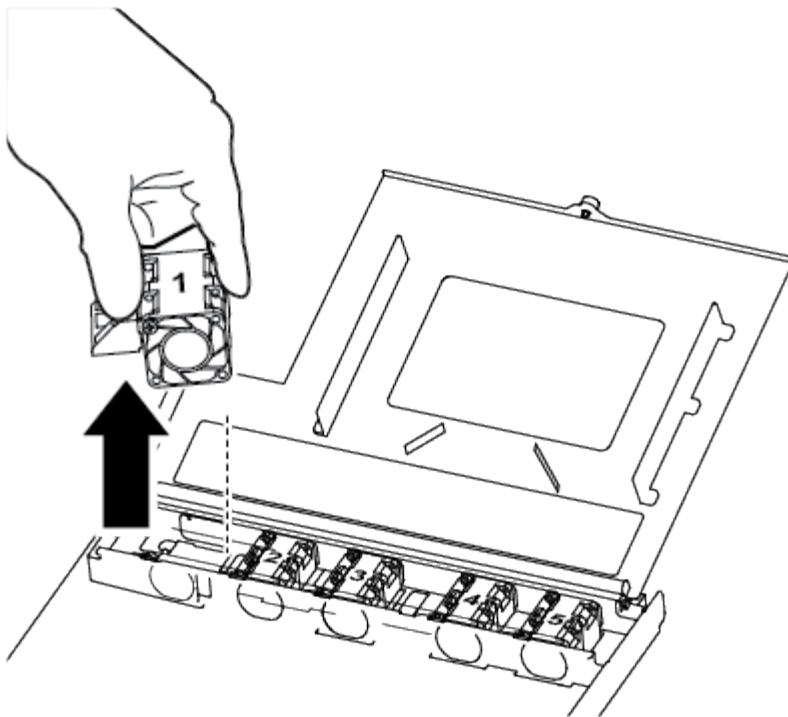
Step 3: Replace a fan

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

Use the following video or the tabulated steps to replace a fan:

[Animation - Replace 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.



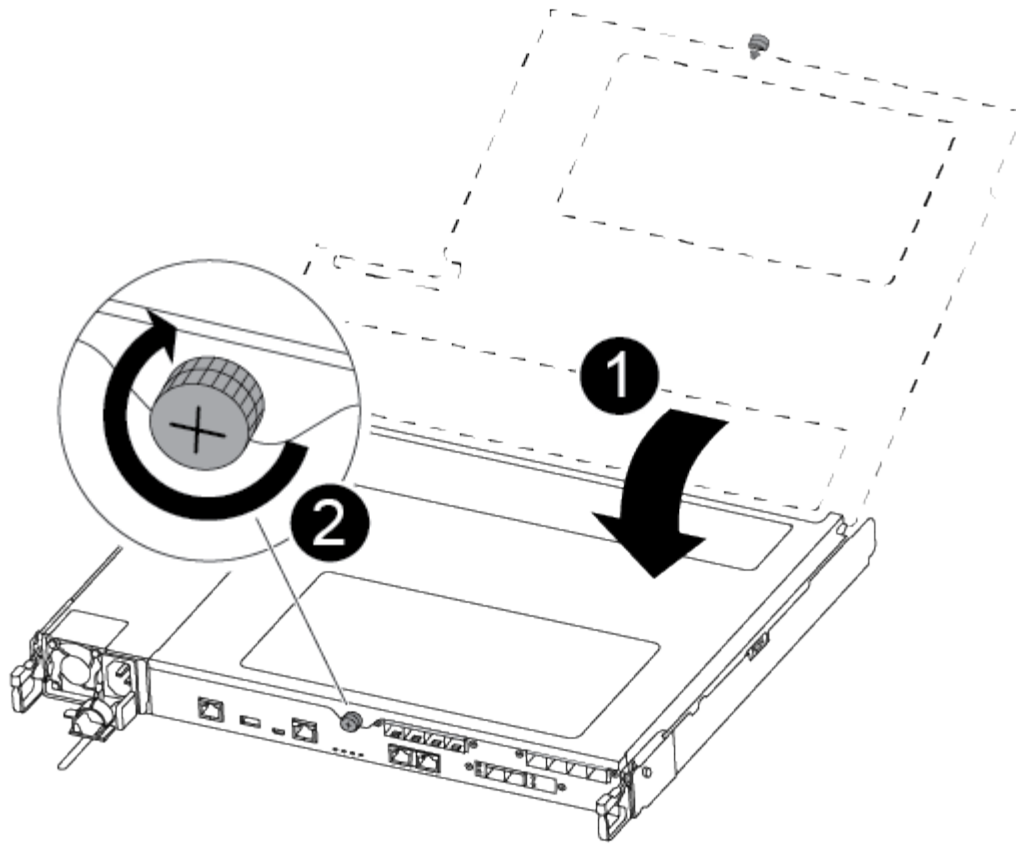
1	Fan module
---	------------

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

- f. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

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 and Replacements](#) page for further information.

Replace or install a mezzanine card - ASA C250

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.

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> The <code>-halt true</code> parameter brings you to the LOADER prompt.

Step 2: Remove the controller module

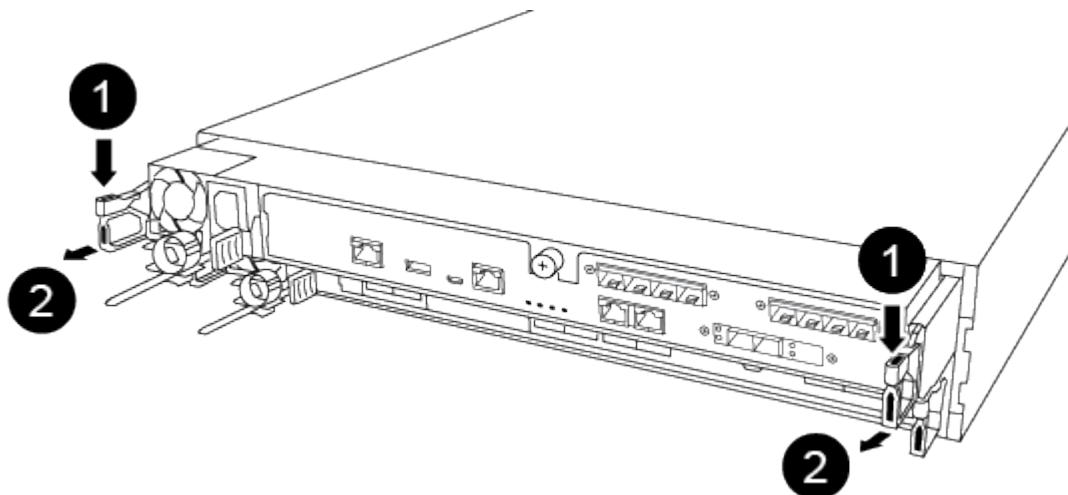
Remove the controller module from the chassis when you replace a component inside the controller module.

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.

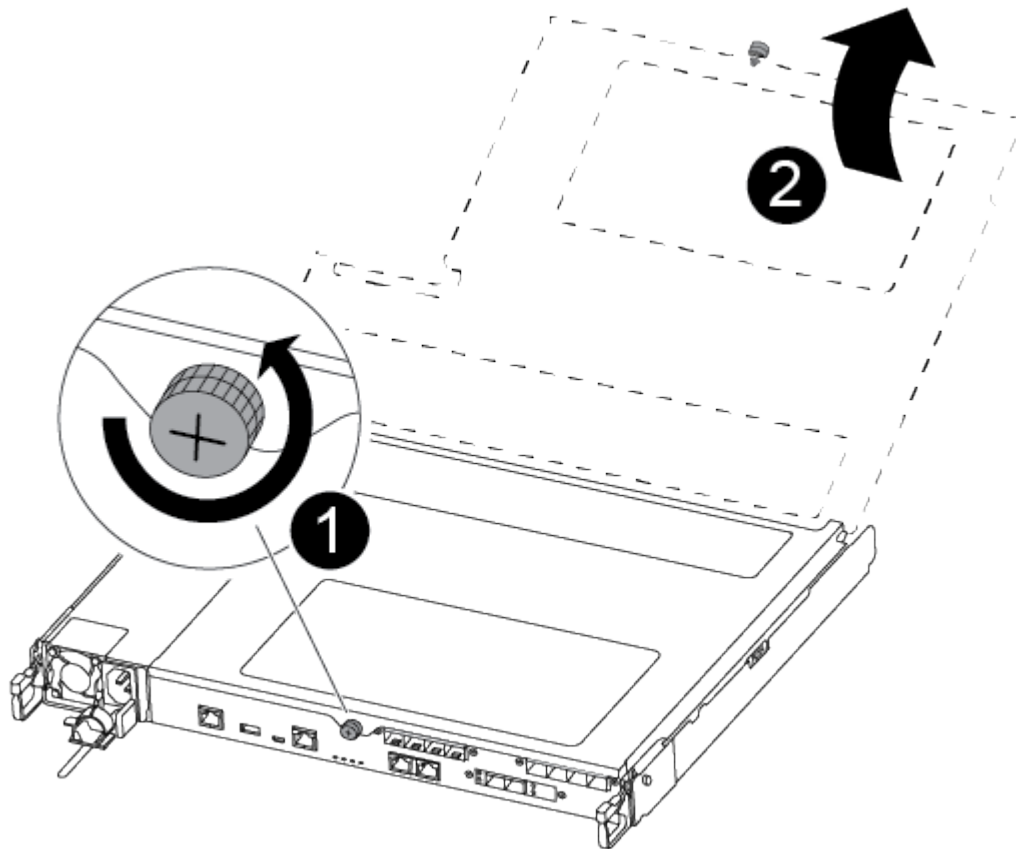


If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



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.

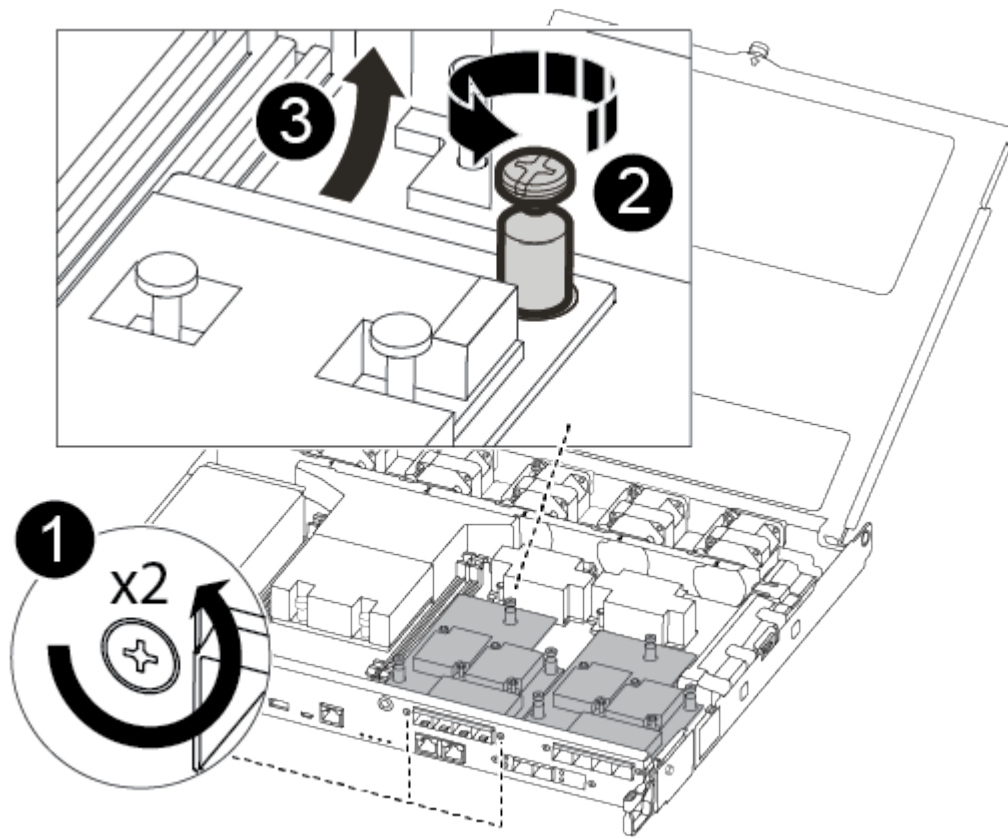
Step 3: Replace or install a mezzanine card

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.

Use the following video or the tabulated steps to replace a mezzanine card:

[Animation - Replace a mezzanine card](#)

1. To replace a mezzanine card:
2. 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.

- a. Unplug any cabling associated with the impaired mezzanine card.

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

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

- h. 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.

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

3. To install a mezzanine card:

4. You install a new mezzanine card if your system does not have one.

- a. 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.
- b. Remove the mezzanine card from the antistatic shipping bag and align it to the inside face of the controller module.
- c. Gently align the mezzanine card into place.
- d. Using the #1 magnetic screwdriver, insert and tighten the screws on the face of the controller module and on the mezzanine card.

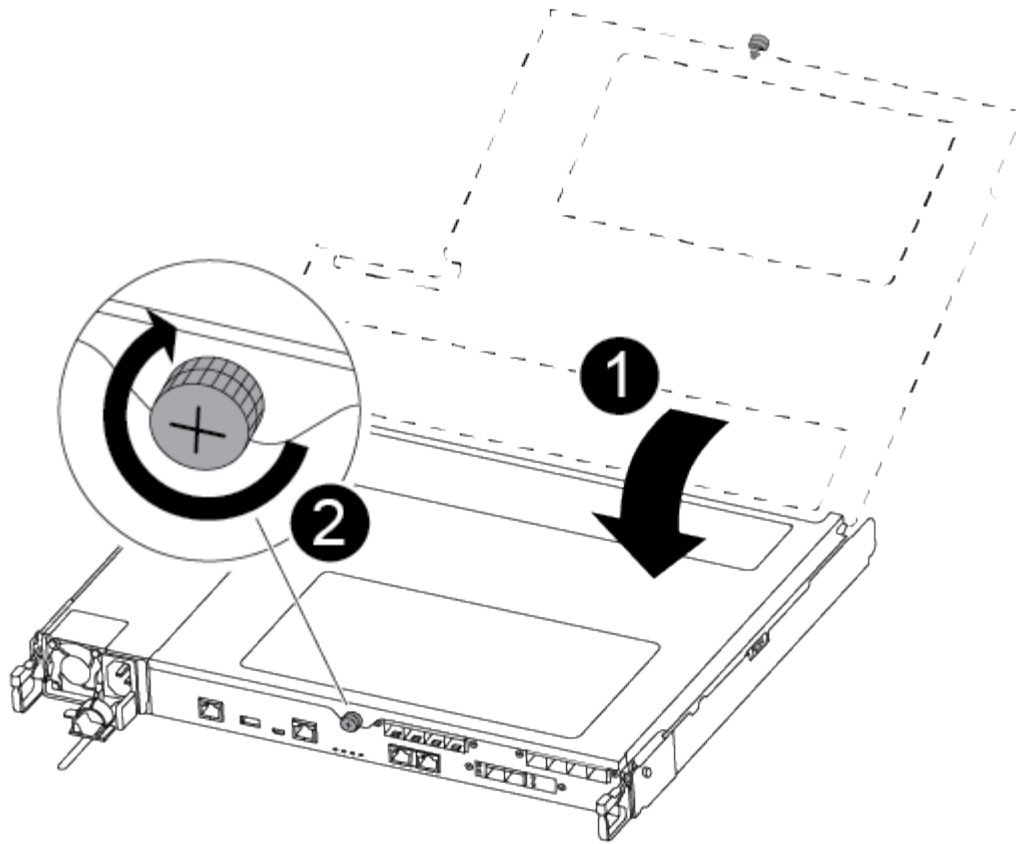


Do not apply force when tightening the screw on the mezzanine card; you might crack it.

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

- f. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

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 and Replacements](#) page for further information.

Replace the NVMEM battery - ASA C250

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <code>-halt true</code> parameter brings you to the LOADER prompt.</p>

Step 2: Remove the controller module

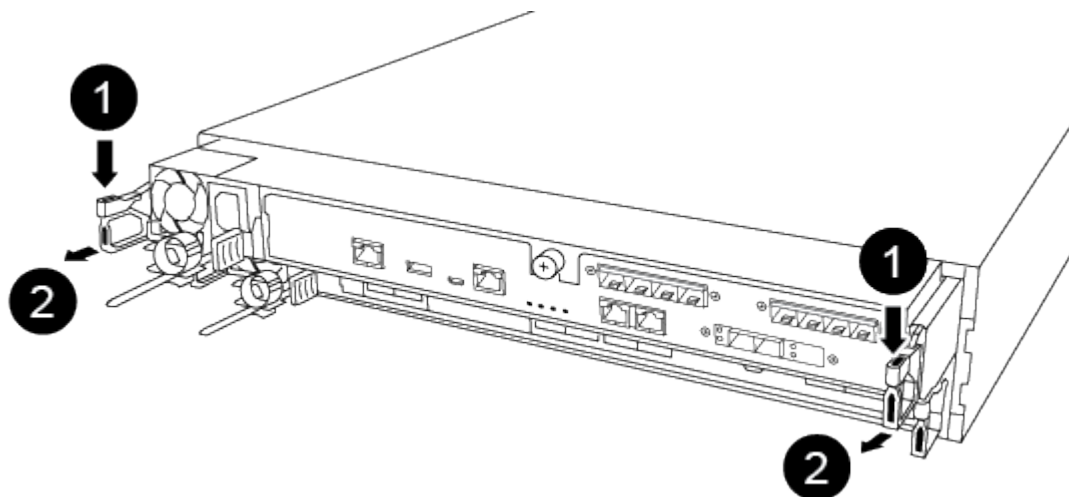
You must remove the controller module from the chassis when you replace a component inside the controller module.

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.



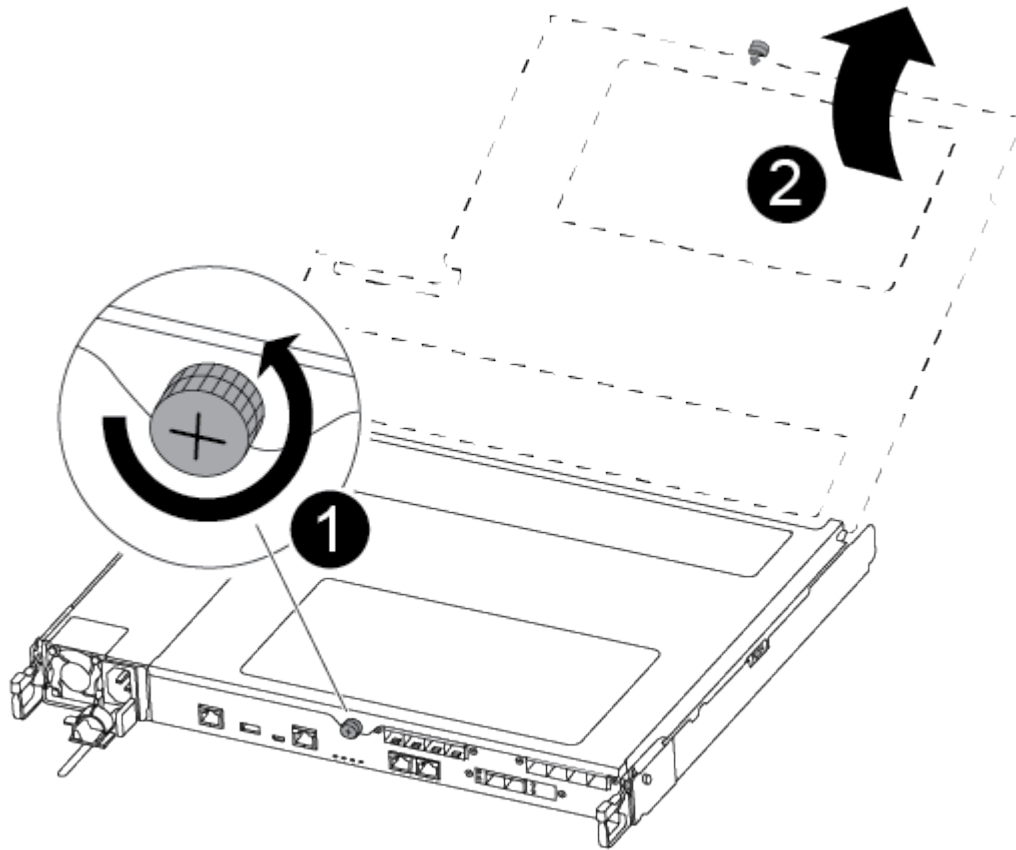
If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



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.

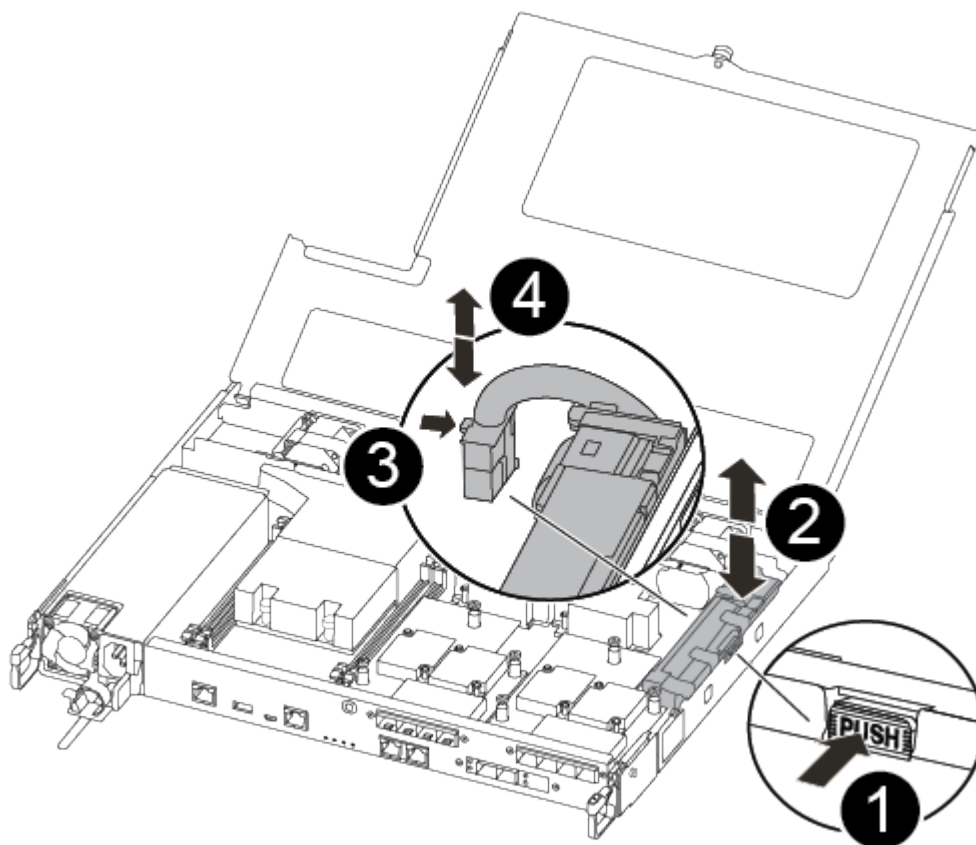
Use the following video or the tabulated steps to replace the NVMEM battery:

[Animation - Replace 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.

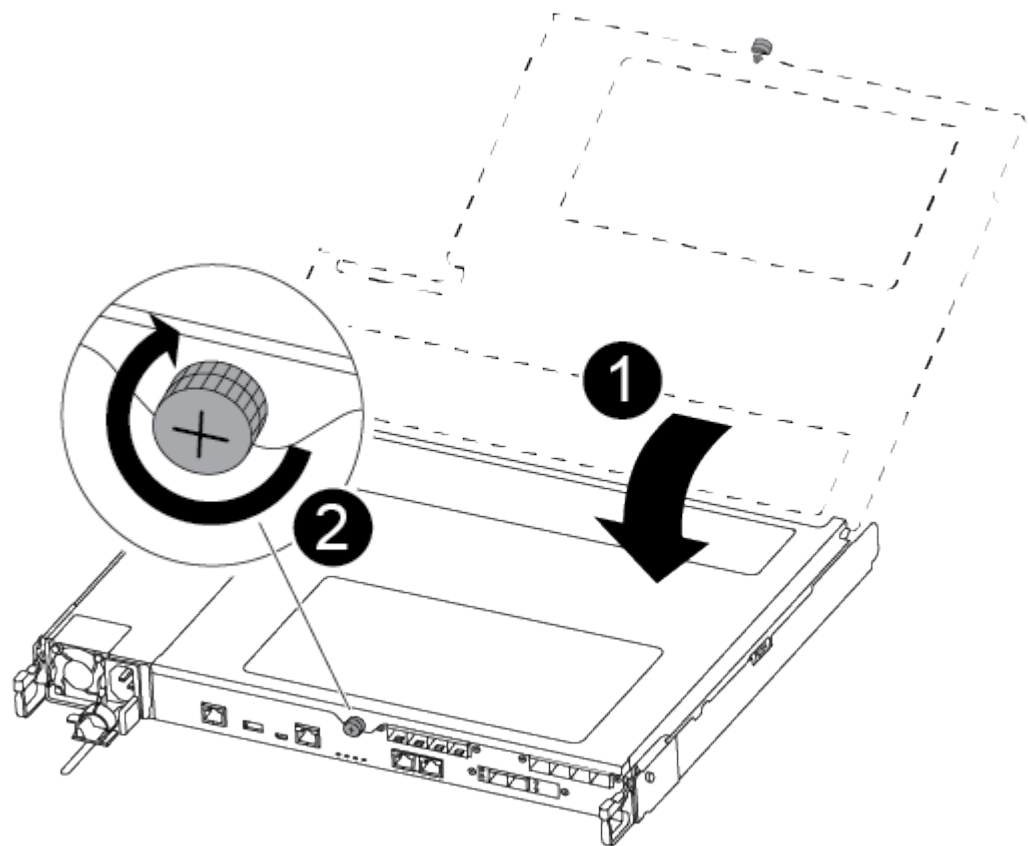
2. Locate the battery plug and squeeze the clip on the face of the battery plug to release the plug from the socket.
3. Grasp the battery and press the blue locking tab marked PUSH, and then lift the battery out of the holder and controller module and set it aside.
4. Remove the replacement NV battery 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.

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

- f. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

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 and Replacements](#) page for further information.

Replace a power supply - ASA C250

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 it to the power source.

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



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

- Power supplies are auto-ranging.



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

Use the appropriate procedure for your type of PSU; AC or DC.

Option 1: Replace an AC PSU

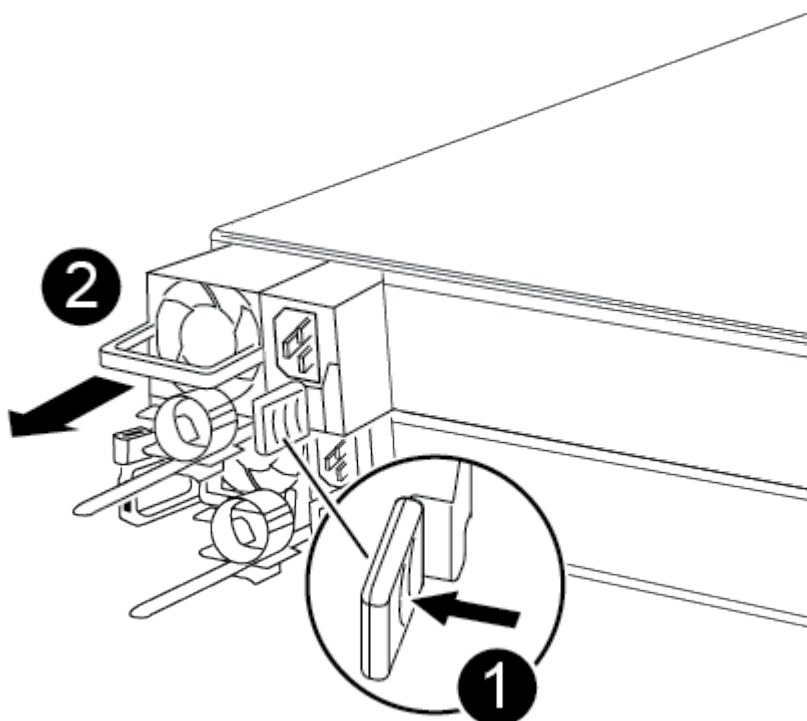
Use the following video or the tabulated steps to replace the PSU:

Animation - Replace the AC PSU

1. If you are not already grounded, properly ground yourself.
2. Identify the PSU you want to replace, based on console error messages or through the red Fault LED on the PSU.
3. Disconnect the PSU:
 - a. Open the power cable retainer, and then unplug the power cable from the PSU.
4. Remove the PSU by rotating the handle up, press the locking tab, and then pull the PSU out of the controller module.



The PSU 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 PSU locking tab
2	Power supply

5. Install the replacement PSU in the controller module:
 - a. Using both hands, support and align the edges of the PSU with the opening in the controller module.

- b. Gently push the PSU 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 PSU into the system.

6. Reconnect the PSU cabling:

- a. Reconnect the power cable to the PSU.
- b. Secure the power cable to the PSU using the power cable retainer.

Once power is restored to the PSU, 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 and Replacements](#) page for further information.

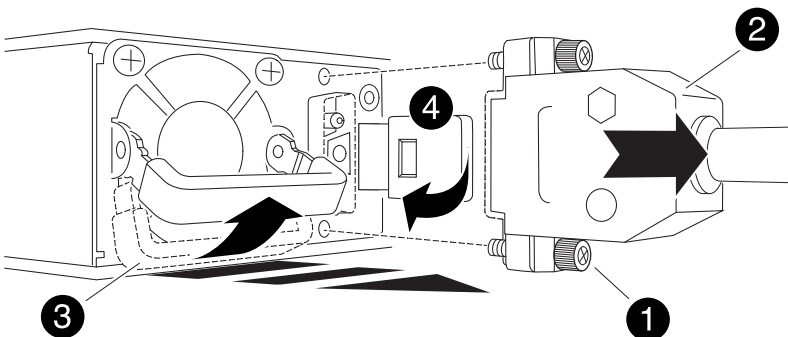
Option 2: Replace a DC PSU

To replace a DC PSU, complete the following steps.

1. If you are not already grounded, properly ground yourself.
2. Identify the PSU you want to replace, based on console error messages or through the red Fault LED on the PSU.
3. Disconnect the PSU:
 - a. Unscrew the D-SUB DC power cable connector using the thumb screws on the plug.
 - b. Unplug the power cable from the PSU and set it aside.
4. Remove the PSU by rotating the handle up, press the locking tab, and then pull PSU out of the controller module.



The PSU 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	Thumb screws
2	D-SUB DC power cable connector

3	Power supply handle
4	Blue PSU locking tab

5. Install the replacement PSU in the controller module:

- a. Using both hands, support and align the edges of the PSU with the opening in the controller module.
- b. Gently push the PSU 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 PSU into the system.

6. Reconnect the D-SUB DC power cable:

- a. Plug the power cable connector into the PSU.
- b. Secure the power cable to the PSU with the thumbscrews.

Once power is restored to the PSU, 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 and Replacements](#) page for further information.

Replace the real-time clock battery - ASA C250

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <code>-halt true</code> parameter brings you to the LOADER prompt.</p>

Step 2: Remove the controller module

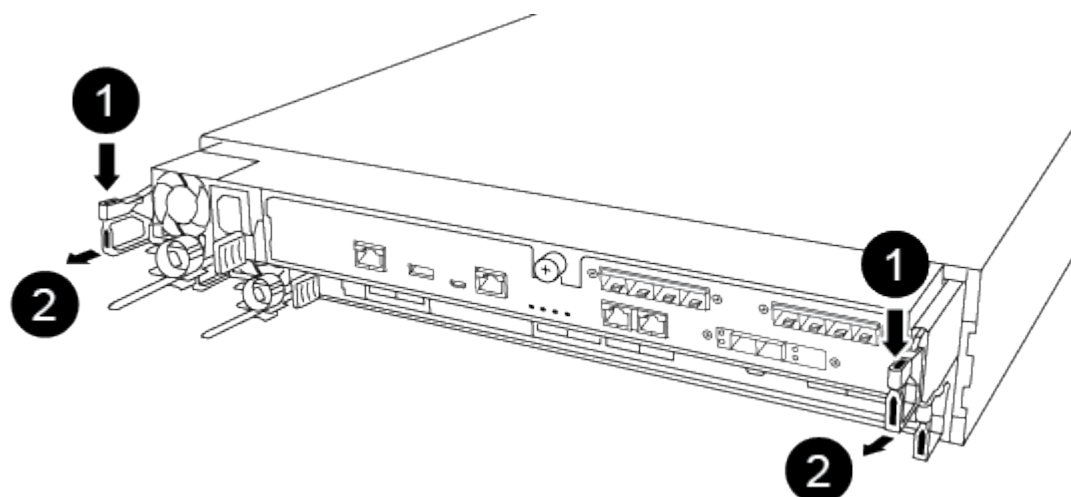
You must remove the controller module from the chassis when you replace a component inside the controller module.

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.

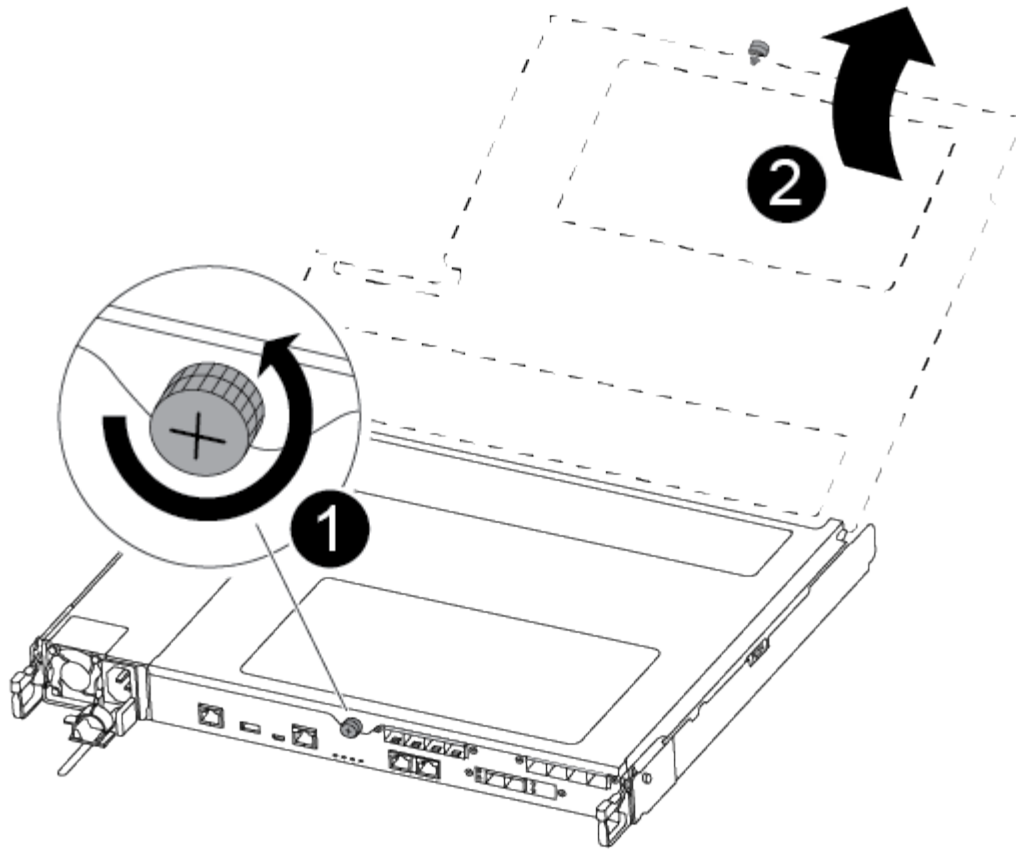


If you have difficulty removing the controller module, place your index fingers through the finger holes from the inside (by crossing your arms).



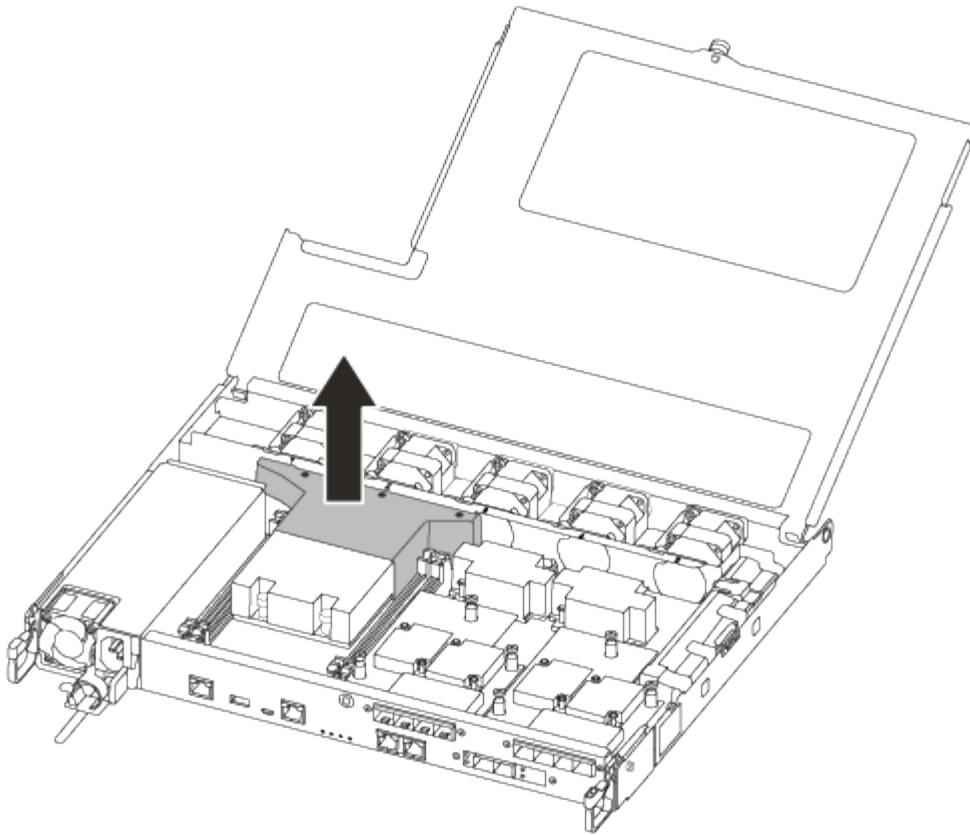
1	Lever
2	Latching mechanism

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.

7. Lift out the air duct cover.



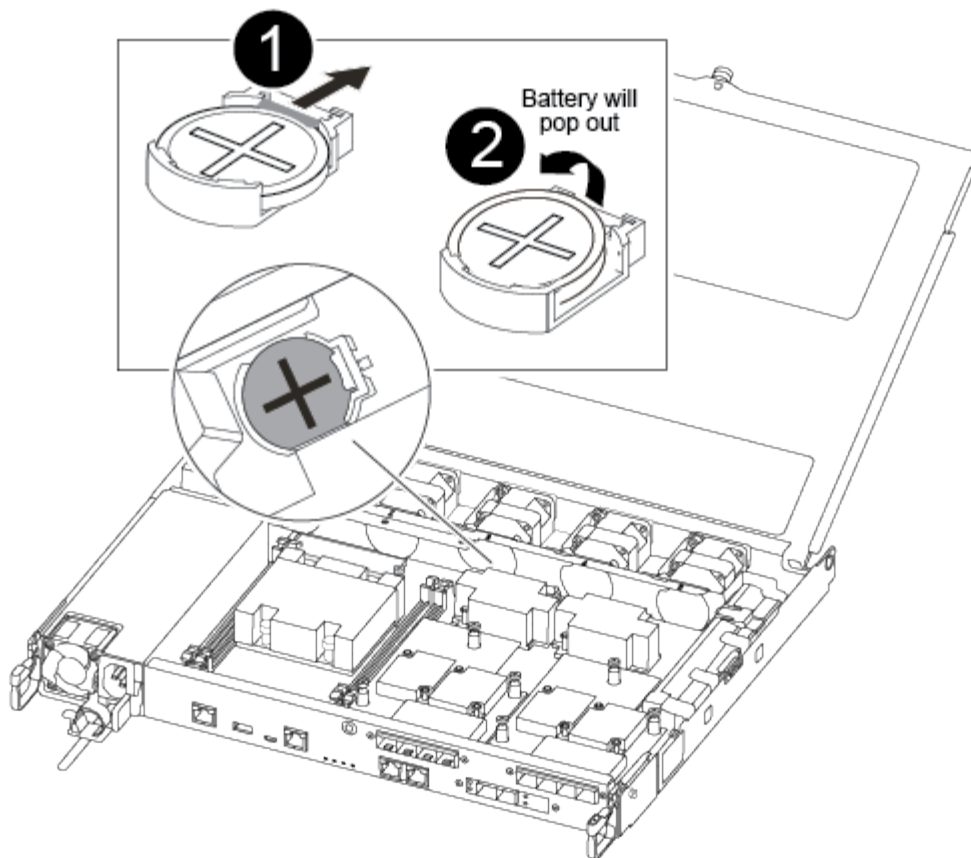
Step 3: Replace the RTC battery

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

Use the following video or the tabulated steps to replace the RTC battery:

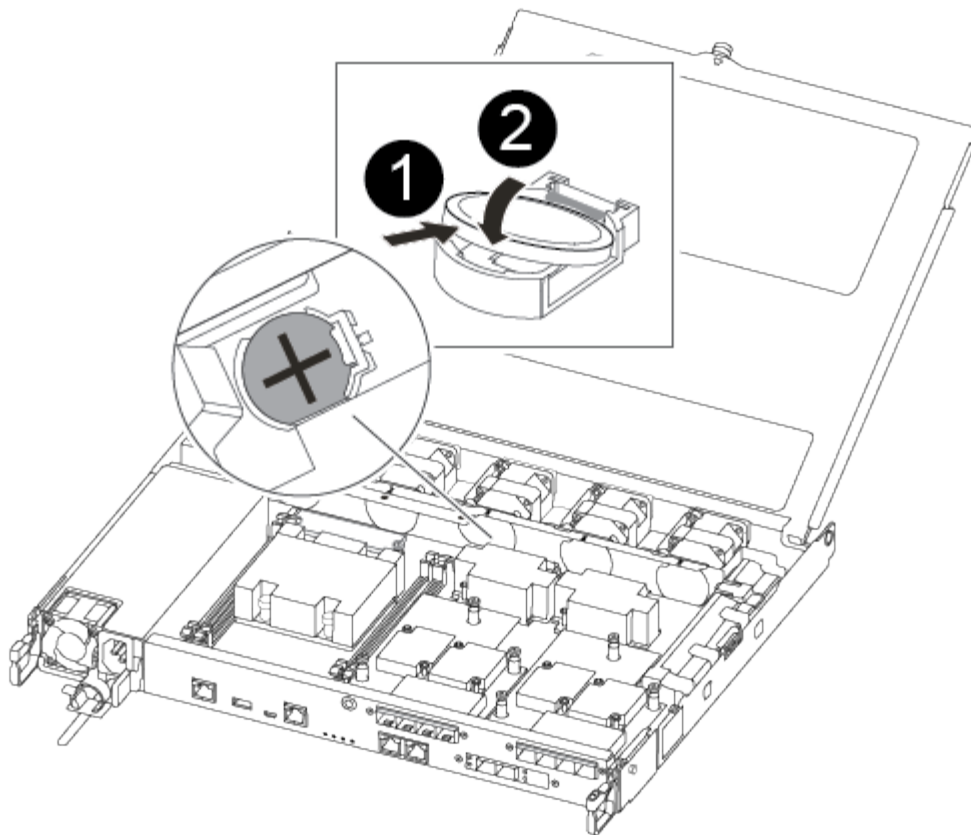
[Animation - Replace the RTC battery](#)


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. Attention: Pulling it away aggressively might displace the tab.
2	Lift the battery up. Note: Make a note of the polarity of the battery.
3	The battery should eject 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.  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 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. 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 should be fully inserted and flush with the edges of the chassis.

- f. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

- g. Halt the controller at the LOADER prompt.

5. 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.

6. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.

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

8. 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 and Replacements](#) page for further information.

ASA C400 systems

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 - ASA C400

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

Use the [AFF C400 Installation and Setup Instructions](#).



The ASA C400 uses the same installation procedure as the AFF C400 system.

Videos - ASA C400

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

[Animation - AFF C400 Installation and setup instructions](#)



The ASA C400 uses the same installation procedure as the AFF C400 system.

If you have a MetroCluster configuration, use the MetroCluster installation content.

[MetroCluster Documentation](#)

Detailed guide - ASA C400

This guide gives detailed step-by-step instructions for installing a typical NetApp system. Use this guide if you want more detailed installation instructions.

If you have a MetroCluster configuration, use the MetroCluster installation content.

[MetroCluster Documentation](#)

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.

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...
100 GbE cable (QSFP28)	X66211A-05 (112-00595), 0.5m X66211A-1 (112-00573), 1m X66211A-2 (112-00574), 2m X66211A-5 (112-00574), 5m		Storage, cluster interconnect/HA, and Ethernet data (order-dependent)
25 GbE cable (SFP28)	X66240-2 (112-00598), 2m X66240-5 (112-00639), 5m		GbE network connection (order-dependent)
32 Gb FC (SFP+ Op)	X66250-2 (112-00342), 2m X66250-5 (112-00344), 5m X66250-15 (112-00346), 15m		FC network connection

Type of cable...	Part number and length	Connector type	For...
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 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 Configuration Guide* and collect the required information listed in that guide.

[ONTAP Configuration Guide](#)

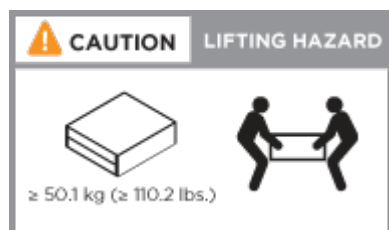
Step 2: Install the hardware

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

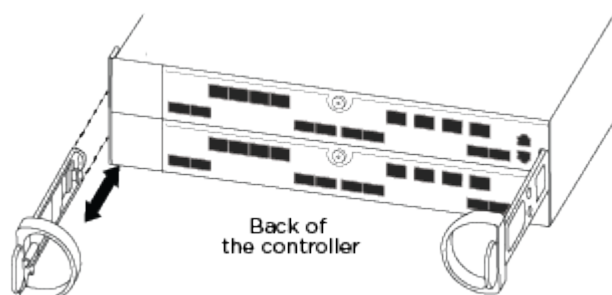
1. Install the rail kits, as needed.
2. Install and secure your system using the instructions included with the rail kit.



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 switched cluster method.

About this task

- If the port labels on the card are not visible, you can identify the ports by checking the card installation orientation (for C400, the PCIe connector socket is on the left side of the card slot), and then look for the card by part number in NetApp Hardware Universe, which shows a graphic of the bezel with the port labels. You can find the card part number using the `sysconfig -a` command or on the system packing list.
- If you are cabling an MetroCluster IP configuration, ports e0a/e0b are available for hosting data LIFs (usually in Default IPspace).

Option 1: Cable a two-node switchless cluster

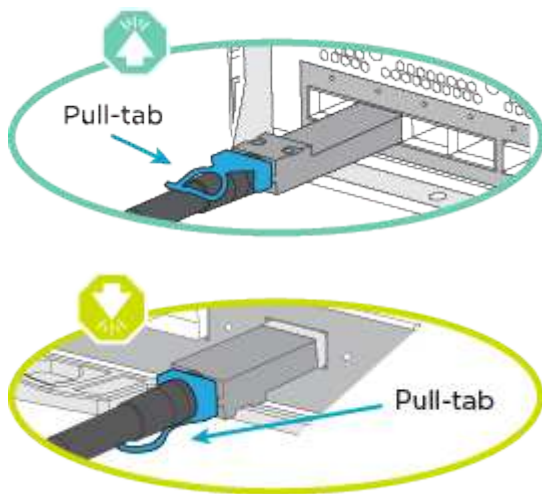
A controller module's cluster interconnect and HA ports are cabled to its partner controller module. The optional data ports, optional NIC cards, and management ports on the controller modules are connected to switches.

Before you begin

You must have contacted your network administrator for information about connecting the system to the switches.

About this task

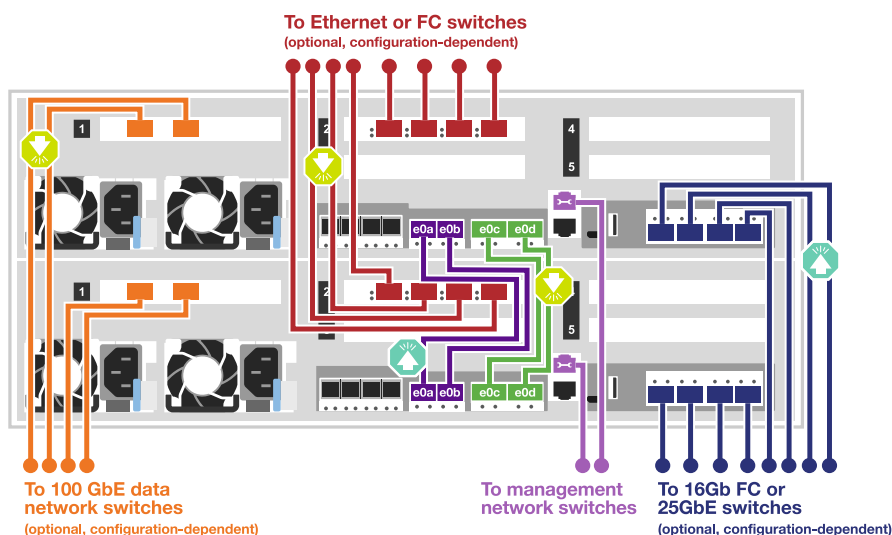
Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all onboard ports and down for expansion (NIC) cards.



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 illustration to complete the cabling between the controllers and the switches:



2. Go to [Step 4: Cable controllers to drive shelves](#) for drive shelf cabling instructions.

Option 2: Cable a switched cluster

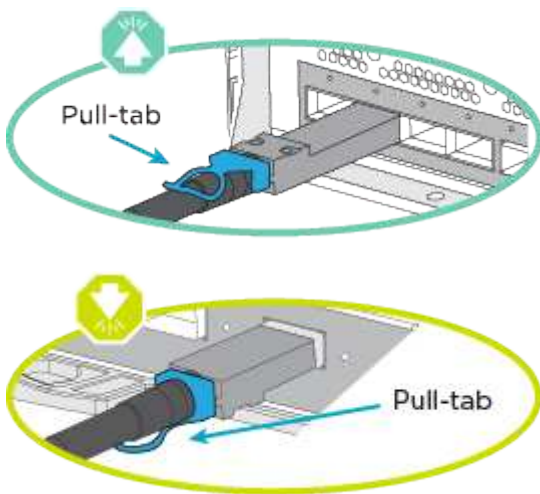
Controller module cluster interconnect and HA ports are cabled to the cluster/HA switch. The optional data ports, optional NIC cards, mezzanine cards, and management ports are connected to switches.

Before you begin

You must have contacted your network administrator for information about connecting the system to the switches.

About this task

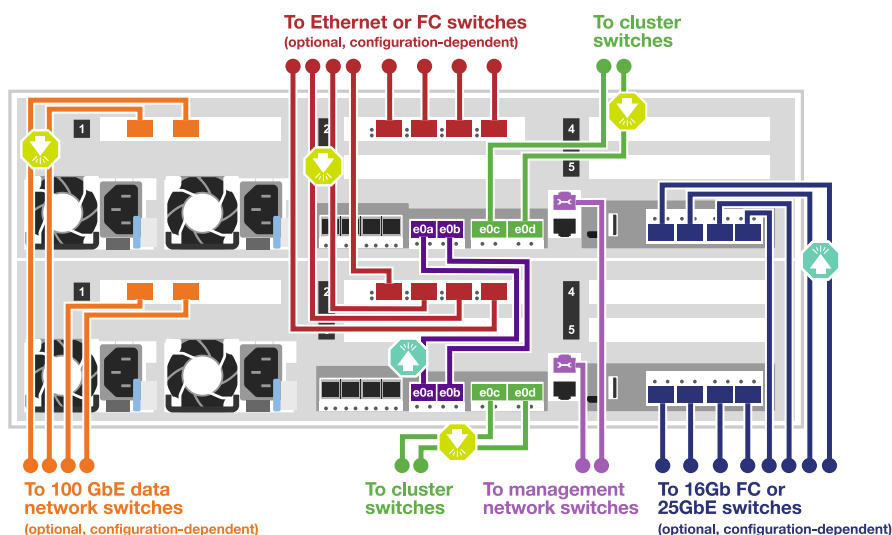
Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all onboard ports and down for expansion (NIC) cards.



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 illustration to complete the cabling between the controllers and the switches:



2. Go to [Step 4: Cable controllers to drive shelves](#) for drive shelf cabling instructions.

Step 4: Cable controllers to drive shelves

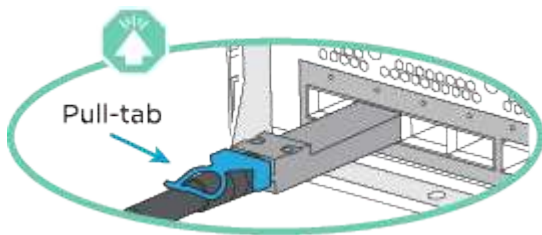
The following options show you how to cable one or two NS224 drive shelves to your system.

Option 1: Cable the controllers to a single drive shelf

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

About this task

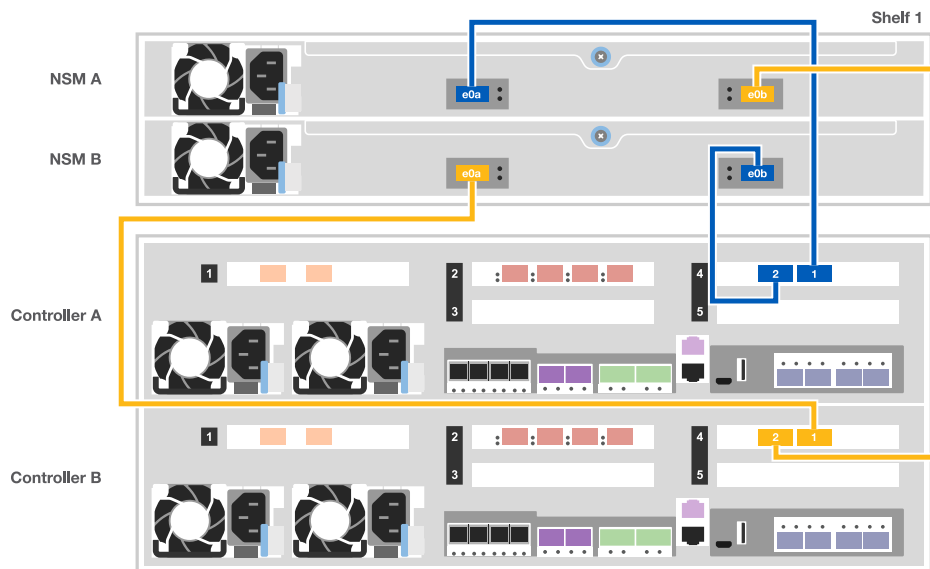
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the NS224 are up.



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 illustration to cable your controllers to a single drive shelf.



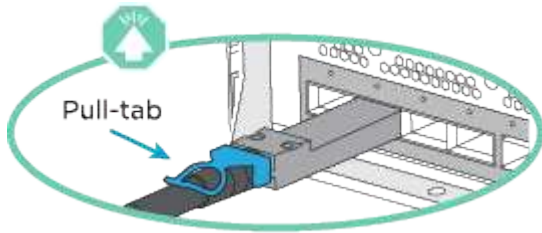
2. Go to [Step 5: Complete system setup and configuration](#) to complete system setup and configuration.

Option 2: Cable the controllers to two drive shelves

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

About this task

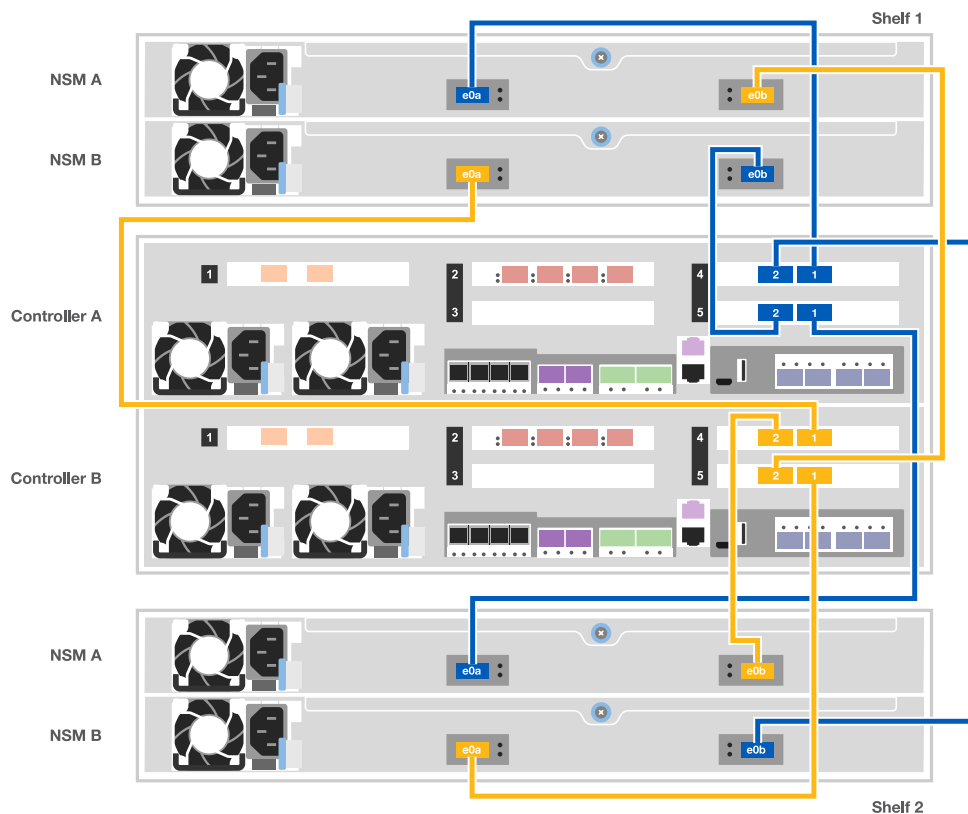
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the NS224 are up.



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 illustration to cable your controllers to two 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.

1. Use the following animation to power on and set shelf IDs for one or more drive shelves:

For NS224 drive shelves, shelf IDs are pre-set to 00 and 01. If you want to change the shelf IDs, use the straightened end of a paperclip, or narrow tipped ball point pen to access the shelf ID button behind the faceplate.

[Animation - Set drive shelf IDs](#)

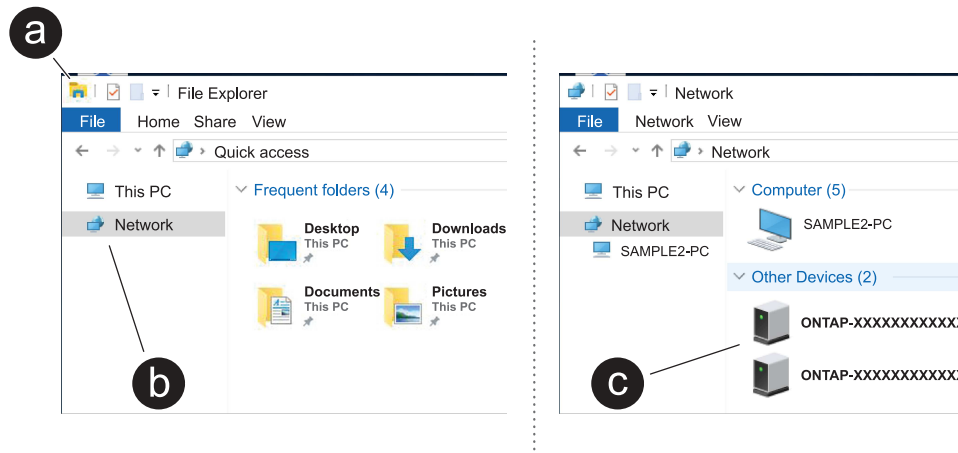
2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Make sure that your laptop has network discovery enabled.

See your laptop's online help for more information.

4. Connect 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 and right-click and select **refresh**.
- c. 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 [ONTAP 9 documentation](#) 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.

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 power on and set shelf IDs for one or more drive shelves:

For NS224 drive shelves, shelf IDs are pre-set to 00 and 01. If you want to change the shelf IDs, use the straightened end of a paperclip, or narrow tipped ball point pen to access the shelf ID button behind the faceplate.

[Animation - Set drive shelf IDs](#)


3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.



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	<p>a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment.</p> <div>  <p>Check your laptop or console's online help if you do not know how to configure PuTTY.</p> </div> <p>b. Enter the management IP address when prompted by the script.</p>

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 [ONTAP 9 documentation](#) for information about configuring additional features in ONTAP.

Maintain

Maintain ASA C400 hardware

Maintain the hardware of your ASA C400 storage system to ensure long-term reliability and optimal performance. Perform regular maintenance tasks such as replacing faulty components, as this helps prevent downtime and data loss.

The maintenance procedures assume that the ASA C400 storage system has already been deployed as a storage node in the ONTAP environment.

System components

For the ASA C400 storage system, you can perform maintenance procedures on the following components.

Boot media - automated recovery	The boot media stores a primary and secondary set of ONTAP image files that the storage system uses to boot. During automated recovery, the system retrieves the boot image from the partner node and automatically runs the appropriate boot menu option to install the image on your replacement boot media. The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the manual boot recovery procedure .
Boot media - manual recovery	The boot media stores a primary and secondary set of ONTAP image files that the storage system uses to boot. During manual recovery, you boot the storage system from a USB drive and manually restore the file system image and configuration. If your storage system is running ONTAP 9.17.1 and later, use the automated boot recovery procedure .
Chassis	The chassis is the physical enclosure housing all the controller components such as the controller/CPU unit, power supply, and I/O.
Controller	A controller consists of a board, firmware, and software. It controls the drives and implements the ONTAP functions.
DIMM	You must replace a DIMM (dual in-line memory module) when a memory mismatch is present, or you have a failed DIMM.
Fan	The fan cools the controller.
NVDIMM	The NVDIMM (non-volatile dual in-line memory module) manages the data transfer from the volatile memory to the non-volatile storage, and maintains data integrity in the event of a power loss or system shutdown.
NVDIMM battery	A NVDIMM battery is responsible for maintaining power to the NVDIMM module.
PCIe card and risers	A PCIe (peripheral component interconnect express) card is an expansion card that plugs into the PCIe slot on the motherboard or into risers plugged into the motherboard.
Power supply	A power supply provides a redundant power source in a controller shelf.
Real-time clock battery	A real time clock battery preserves system date and time information if the power is off.

Boot media - automated recovery

Boot media automated recovery workflow - ASA C400

The automated recovery of the boot image involves the system automatically identifying and selecting the appropriate boot menu option. It uses the boot image on partner node to reinstall ONTAP on the replacement boot media in your ASA C400 storage system.

The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the [manual boot recovery procedure](#).

To get started, review the replacement requirements, shut down the controller, replace the boot media, allow the system to restore the image, and verify system functionality.

1

Review the boot media requirements

Review the requirements for boot media replacement.

2

Shut down the controller

Shut down the controller in your storage system when when you need to replace the boot media.

3

Replace the boot media

Remove the failed boot media from the controller module and install the replacement boot media.

4

Restore the image on the boot media

Restore the ONTAP image from the partner controller.

5

Return the failed part to NetApp

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

Requirements for automated boot media recovery - ASA C400

Before replacing the boot media in your ASA C400, ensure you meet the necessary requirements for a successful replacement. This includes verifying that you have the correct replacement boot media, confirming that the e0S (e0M wrench) port on the impaired controller is not faulty, and determining whether Onboard Key Manager (OKM) or External Key Manager (EKM) is enabled.

The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the [manual boot recovery procedure](#).

- You must replace the failed component with a replacement FRU component of the same capacity that you received from NetApp.
- Verify that the e0M (wrench) port on the impaired controller is connected and not faulty.

The e0M port is used to communicate between the two controllers during the automated boot recovery

process.

- For OKM, you need the cluster-wide passphrase and also the backup data.
- For EKM, you need copies of the following files from the partner node:
 - /cfcard/kmip/servers.cfg file.
 - /cfcard/kmip/certs/client.crt file.
 - /cfcard/kmip/certs/client.key file.
 - /cfcard/kmip/certs/CA.pem file.
- It is critical to apply the commands to the correct controller when you are replacing the impaired boot media:
 - The *impaired controller* is the controller on which you are performing maintenance.
 - The *healthy controller* is the HA partner of the impaired controller.

What's next

After you've reviewed the boot media requirements, you [shut down the controller](#).

Shut down the controller for automated boot media recovery - ASA C400

Shut down the impaired controller in your ASA C400 storage system to prevent data loss and maintain system stability during the automated boot media recovery process.

The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the [manual boot recovery procedure](#).

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> The <code>-halt true</code> parameter brings you to the LOADER prompt.

What's next

After you shut down the impaired controller, you [replace the boot media](#).

Replace the boot media for automated boot recovery - ASA C400

The boot media in your ASA C400 system stores essential firmware and configuration data. The replacement process involves removing and opening the controller module, removing the impaired boot media, installing the replacement boot media in the controller module, and then reinstalling the controller module.

The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the [manual boot recovery procedure](#).

The boot media is located inside the controller module under the air duct, and is accessed by removing the controller module from the system.

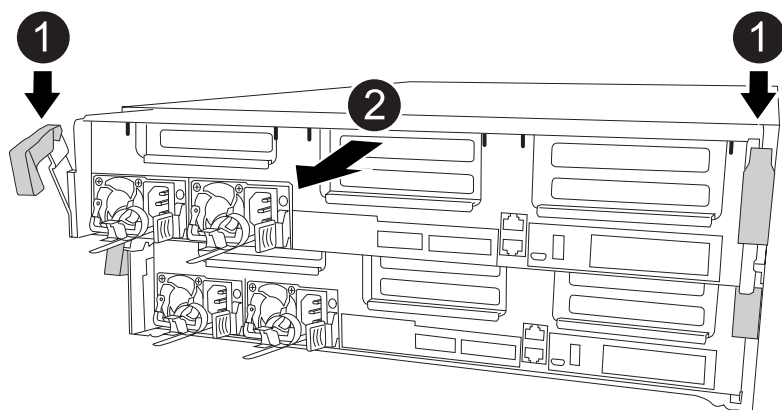
Steps

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.



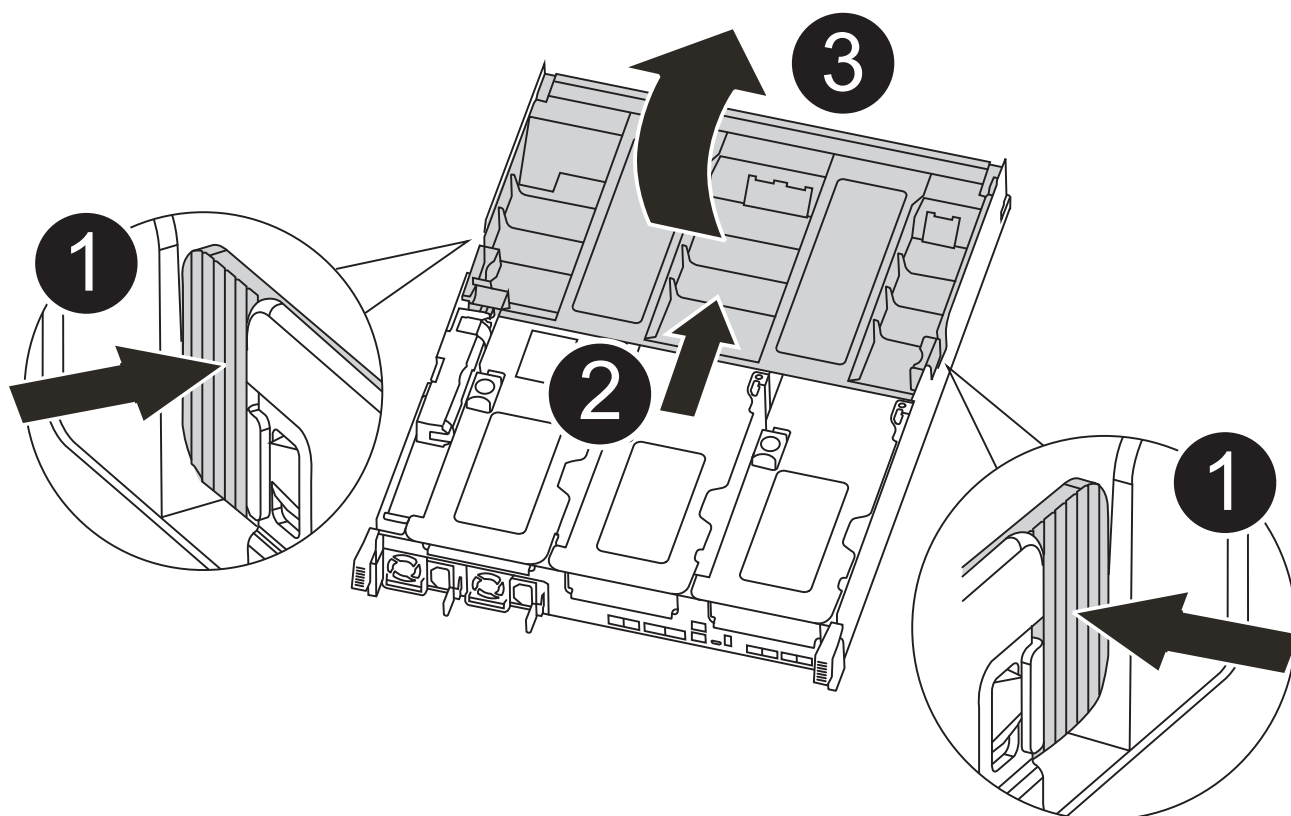
1	Locking latches
2	Controller moves slightly out of chassis

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.

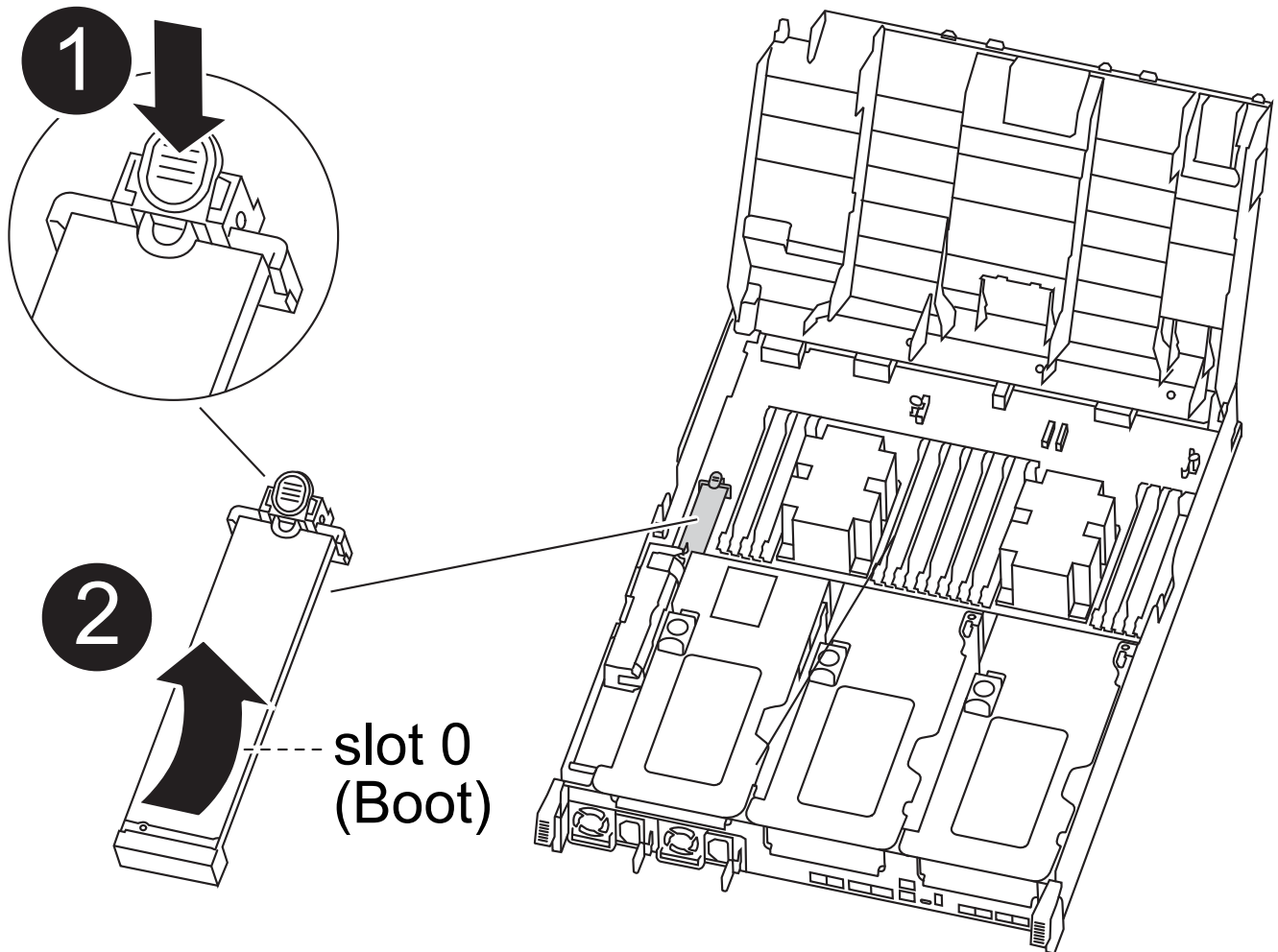
8. Open the air duct:



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.

9. 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.
10. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket.
11. Check the boot media to make sure that it is seated squarely and completely in the socket.

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

12. 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.
13. Close the air duct.

What's next

After physically replacing the impaired boot media, [restore the ONTAP image from the partner node](#).

Automated boot media recovery from the partner node - ASA C400

After installing the new boot media device in your ASA C400 system, you can start the automated boot media recovery process to restore the configuration from the partner node. During the recovery process, the system checks whether encryption is enabled and determines the type of key encryption in use. If key encryption is enabled, the system guides you through the appropriate steps to restore it.

The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the [manual boot recovery procedure](#).

Before you begin

- For OKM, you need the cluster-wide passphrase and also the backup data.
- For EKM, you need copies of the following files from the partner node:
 - /cfcard/kmip/servers.cfg file.
 - /cfcard/kmip/certs/client.crt file.
 - /cfcard/kmip/certs/client.key file.
 - /cfcard/kmip/certs/CA.pem file.

Steps

1. From the LOADER prompt, enter the command:

```
boot_recovery -partner
```

The screen displays the following message:

```
Starting boot media recovery (BMR) process. Press Ctrl-C to abort...
```

2. Monitor the boot media install recovery process.

The process completes and displays the `Installation complete` message.

3. The system checks for encryption and encryption type and displays one of two messages. Depending on what message is displayed, take one of the following actions:



Occasionally, the process may not be able to identify if key manager is configured on the system. It will display an error message, ask if key manager is configured for the system, and then ask what type of key manager is configured. The process will resume after you resolve the issue.

Show example of configuration error finding prompts

```
Error when fetching key manager config from partner ${partner_ip}:  
${status}
```

```
Has key manager been configured on this system
```

```
Is the key manager onboard
```

If you see this message...	Do this...
key manager is not configured. Exiting.	<p>Encryption is not installed on the system. Complete the following steps:</p> <ol style="list-style-type: none">Log into the node when the login prompt is displayed and give back the storage: <pre>storage failover giveback -ofnode impaired_node_name</pre>Go to step 5 to enable automatic giveback if it was disabled.
key manager is configured.	<p>Go to step 4 to restore the appropriate key manager.</p> <p>The node accesses the boot menu and runs:</p> <ul style="list-style-type: none">Option 10 for systems with Onboard Key Manager (OKM).Option 11 for systems with External Key Manager (EKM).

4. Select the appropriate key manager restoration process.

Onboard Key Manager (OKM)

If OKM is detected, the system displays the following message and begins running BootMenu Option 10.

```
key manager is configured.  
Entering Bootmenu Option 10...
```

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

- a. Enter `y` at the prompt to confirm you want to start the OKM recovery process.
- b. Enter the following when prompted:
 - i. The passphrase
 - ii. The passphrase again when prompted to confirm
 - iii. Backup data for onboard key manager

Show example of passphrase and backup data prompts

```
Enter the passphrase for onboard key management:  
-----BEGIN PASSPHRASE-----  
<passphrase_value>  
-----END PASSPHRASE-----  
Enter the passphrase again to confirm:  
-----BEGIN PASSPHRASE-----  
<passphrase_value>  
-----END PASSPHRASE-----  
Enter the backup data:  
-----BEGIN BACKUP-----  
<passphrase_value>  
-----END BACKUP-----
```

- c. Continue to monitor the recovery process as it restores the appropriate files from the partner node.

When the recovery process is complete, the node will reboot. The following messages indicate a successful recovery:

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

Successfully recovered keymanager secrets.
```

d. When the node reboots, verify the boot media recovery was successful by confirming that the system is back online and operational.

e. Return the impaired controller to normal operation by giving back its storage:

```
storage failover giveback -ofnode impaired_node_name
```

f. After the partner node is fully up and serving data, synchronize the OKM keys across the cluster.

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

External Key Manager (EKM)

If EKM is detected, the system displays the following message and begins running BootMenu Option 11.

```
key manager is configured.
Entering Bootmenu Option 11...
```

a. The next step depends on which version of ONTAP your system is running:

If your system is running...	Do this...
ONTAP 9.16.0	<p>a. Press <code>Ctrl-C</code> to exit BootMenu Option 11.</p> <p>b. Press <code>Ctrl-C</code> to exit the EKM configuration process and return to the boot menu.</p> <p>c. Select BootMenu Option 8.</p> <p>d. Reboot the node.</p> <p>If AUTOBOOT is set, the node reboots and uses the configuration files from the partner node.</p> <p>If AUTOBOOT is not set, enter the appropriate boot command. The node reboots and uses the configuration files from the partner node.</p> <p>e. Reboot the node so that EKM protects the boot media partition.</p> <p>f. Proceed to step c.</p>

If your system is running...	Do this...
ONTAP 9.16.1 and later	Proceed to the next step.

b. Enter the following EKM configuration setting when prompted:

Action	Example
Enter the client certificate contents from the /cfcard/kmip/certs/client.crt file.	Show example of client certificate contents <pre> -----BEGIN CERTIFICATE----- <certificate_value> -----END CERTIFICATE----- </pre>
Enter the client key file contents from the /cfcard/kmip/certs/client.key file.	Show example of client key file contents <pre> -----BEGIN RSA PRIVATE KEY----- <key_value> -----END RSA PRIVATE KEY----- </pre>
Enter the KMIP server CA(s) file contents from the /cfcard/kmip/certs/CA.pem file.	Show example of KMIP server file contents <pre> -----BEGIN CERTIFICATE----- <KMIP_certificate_CA_value > -----END CERTIFICATE----- </pre>

Action	Example
<p>Enter the server configuration file contents from the /cfcard/kmip/servers.cfg file.</p>	<p>Show example of server configuration file contents</p> <pre> xxx.xxx.xxx.xxx:5696.host= xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx:5696.port= 5696 xxx.xxx.xxx.xxx:5696.trust ed_file=/cfcard/kmip/certs /CA.pem xxx.xxx.xxx.xxx:5696.proto col=KMIP1_4 1xxx.xxx.xxx.xxx:5696.time out=25 xxx.xxx.xxx.xxx:5696.nbio= 1 xxx.xxx.xxx.xxx:5696.cert_ file=/cfcard/kmip/certs/cl ient.crt xxx.xxx.xxx.xxx:5696.key_f ile=/cfcard/kmip/certs/cli ent.key xxx.xxx.xxx.xxx:5696.ciphe rs="TLSv1.2:kRSA:!CAMELLIA :!IDEA:!RC2:!RC4:!SEED:!eN ULL:!aNULL" xxx.xxx.xxx.xxx:5696.verif y=true xxx.xxx.xxx.xxx:5696.netap p_keystore_uuid=<id_value> </pre>

Action	Example
<p>If prompted, enter the ONTAP Cluster UUID from the partner.</p> <p>You can check the cluster UUID from the partner node using the <code>cluster identify show</code> command.</p>	<p>Show example of ONTAP Cluster UUID</p> <div data-bbox="898 233 1425 730"> <p>Notice:</p> <pre>bootarg.mgwd.cluster_uuid is not set or is empty. Do you know the ONTAP Cluster UUID? {y/n} y Enter the ONTAP Cluster UUID: <cluster_uuid_value></pre> <p>System is ready to utilize external key manager(s).</p> </div>
<p>If prompted, enter the temporary network interface and settings for the node.</p> <p>You need to enter:</p> <ol style="list-style-type: none"> 1. The IP address for the port 2. The netmask for the port 3. The IP address of the default gateway 	<p>Show example of a temporary network setting</p> <div data-bbox="898 884 1425 1864"> <p>In order to recover key information, a temporary network interface needs to be configured.</p> <p>Select the network port you want to use (for example, 'e0a')</p> <pre>e0M</pre> <p>Enter the IP address for port : xxx.xxx.xxx.xxx</p> <p>Enter the netmask for port : xxx.xxx.xxx.xxx</p> <p>Enter IP address of default gateway: xxx.xxx.xxx.xxx</p> <p>Trying to recover keys from key servers....</p> <pre>[discover_versions] [status=SUCCESS reason=message=]</pre> </div>

c. Depending on whether the key is successfully restored, take one of the following actions:

- If you see `kmip2_client: Successfully imported the keys from external key server: xxx.xxx.xxx.xxx:5696` in the output, the EKM configuration has been successfully restored.

The process attempts to restore the appropriate files from the partner node and reboots the node. Go to step d.

- If the key is not successfully restored, the system will halt and indicate that it could not restore the key. The error and warning messages are displayed. You must rerun the recovery process:

```
boot_recovery -partner
```

Show example of key recovery error and warning messages

```
ERROR: kmip_init: halting this system with encrypted
mroot...
WARNING: kmip_init: authentication keys might not be
available.
*****
*                               A T T E N T I O N                               *
*                                                                                   *
*          System cannot connect to key managers.          *
*                                                                                   *
*****
ERROR: kmip_init: halting this system with encrypted
mroot...
.
Terminated

Uptime: 11m32s
System halting...

LOADER-B>
```

d. When the node reboots, verify that the boot media recovery was successful by confirming that the system is back online and operational.

e. 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
```

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

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

What's next

After you've restored the ONTAP image and the node is up and serving data, you [return the failed part to NetApp](#).

Return the failed boot media to NetApp - ASA C400

If a component in your ASA C400 system fails, return the failed part to NetApp. See the [Part Return and Replacements](#) page for further information.

Boot media - manual recovery

Boot media manual recovery workflow - ASA C400

Get started with replacing the boot media in your ASA C400 storage system by reviewing the replacement requirements, checking encryption status, shutting down the controller, replacing the boot media, booting the recovery image, restoring encryption, and verifying the system functionality.

If your storage system is running ONTAP 9.17.1 or later, use the [automated boot recovery procedure](#). If your system is running an earlier version of ONTAP, you must use the manual boot recovery process.

1

Review the boot media requirements

Review the requirements for replacing the boot media.

2

Check encryption key support and status

Determine whether the system has security key manager enabled or encrypted disks.

3

Shut down the controller

Shut down the controller when you need to replace the boot media.

4

Replace the boot media

Remove the failed boot media from the System Management module and install the replacement boot media, and then transfer an ONTAP image using a USB flash drive.

5

Boot the recovery image

Boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

6

Restore encryption

Restore the onboard key manager configuration or the external key manager from the ONATP boot menu.

7

Return the failed part to NetApp

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

Requirements for manual boot media recovery - ASA C400

Before replacing the boot media in your ASA C400 system, ensure you meet the necessary requirements for a successful replacement. This includes making sure you have a USB flash drive with the appropriate amount of storage and verifying that you have the correct replacement boot device.

If your storage system is running ONTAP 9.17.1 or later, use the [automated boot recovery procedure](#). If your system is running an earlier version of ONTAP, you must use the manual boot recovery process.

What's next?

After you've reviewed the requirements to replace the boot media, you need to [check encryption key support and status on the boot media](#).

Check encryption key support and status - ASA C400

To ensure data security on your storage system, you need to verify the encryption key support and status on your boot media. Check if your ONTAP version supports NetApp Volume Encryption (NVE), and before you shut down the controller check if the key manager is active.

If your storage system is running ONTAP 9.17.1 or later, use the [automated boot recovery procedure](#). If your system is running an earlier version of ONTAP, you must use the manual boot recovery process.

Step 1: Check if your version of ONTAP supports NetApp Volume Encryption

Check whether your ONTAP version supports NetApp Volume Encryption (NVE). This information is crucial for downloading the correct ONTAP image.

Steps

1. Determine if your ONTAP version supports encryption by running the following command:

```
version -v
```

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

2. Depending on whether NVE is supported on your system, take one of the following actions:
 - If NVE is supported, download the ONTAP image with NetApp Volume Encryption.
 - If NVE is not supported, download the ONTAP image **without** NetApp Volume Encryption.

Step 2: Determine if it is safe to shut down the controller

To safely shut down a controller, first identify whether the External Key Manager (EKM) or the Onboard Key Manager (OKM) is active. Then, verify the key manager in use, display the appropriate key information, and take action based on the status of the authentication keys.

Steps

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

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

2. Depending on whether a key manger is configured on your system, select one of the following options.

No key manager configured

You can safely shut down the impaired controller. Go to [shutdown the impaired controller](#).

External or Onboard key manager configured

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

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

- b. Check the output for the value in the `Restored` column for your key manager.

This column indicates whether the authentication keys for your key manager (either EKM or OKM) have been successfully restored.

3. Depending on whether your system is using the External Key Manager or Onboard Key Manager, select one of the following options.

External Key Manager

Depending on the output value displayed in the `Restored` column, follow the appropriate steps.

Output value in <code>Restored</code> column	Follow these steps...
true	You can safely shut down the impaired controller. Go to shutdown the impaired controller .
Anything other than true	<p>a. Restore the external key management authentication keys to all nodes in the cluster using the following command:</p> <pre>security key-manager external restore</pre> <p>If the command fails, contact NetApp Support.</p> <p>b. Verify that the <code>Restored</code> column displays <code>true</code> for all authentication keys by entering the <code>security key-manager key query</code> command.</p> <p>If all the authentication keys are <code>true</code>, you can safely shut down the impaired controller. Go to shutdown the impaired controller.</p>

Onboard Key Manager

Depending on the output value displayed in the `Restored` column, follow the appropriate steps.

Output value in <code>Restored</code> column	Follow these steps...
true	<p>Manually back up the OKM information.</p> <p>a. Go to the advanced mode by entering <code>set -priv advanced</code> and then enter <code>Y</code> when prompted.</p> <p>b. Enter the following command to display the key management information:</p> <pre>security key-manager onboard show-backup</pre> <p>c. Copy the contents of the backup information to a separate file or your log file.</p> <p>You'll need it in disaster scenarios where you might need to manually recover OKM.</p> <p>d. You can safely shut down the impaired controller. Go to shutdown the impaired controller.</p>

Output value in Restored column	Follow these steps...
Anything other than true	<p>a. Enter the onboard security key-manager sync command:</p> <pre>security key-manager onboard sync</pre> <p>b. Enter the 32 character, alphanumeric onboard key management passphrase when prompted.</p> <p>If the passphrase cannot be provided, contact NetApp Support.</p> <p>c. Verify the Restored column displays true for all authentication keys:</p> <pre>security key-manager key query</pre> <p>d. Verify that the Key Manager type displays onboard, and then manually back up the OKM information.</p> <p>e. Enter the command to display the key management backup information:</p> <pre>security key-manager onboard show-backup</pre> <p>f. Copy the contents of the backup information to a separate file or your log file.</p> <p>You'll need it in disaster scenarios where you might need to manually recover OKM.</p> <p>g. You can safely shut down the impaired controller. Go to shutdown the impaired controller.</p>

Shut down the controller for manual boot media recovery - ASA C400

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.

If your storage system is running ONTAP 9.17.1 or later, use the [automated boot recovery procedure](#). If your system is running an earlier version of ONTAP, you must use the manual boot recovery process.

Option 1: Most configurations

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

Steps

- Take the impaired controller to the LOADER prompt:

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

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



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

Option 2: Controller is in a MetroCluster 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 [Synchronize a node with the cluster](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

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

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

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

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

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

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

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

Option 3: Controller is in a two-node Metrocluster

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

About this task

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

Steps

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

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

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

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes

that prevent the healing operation.

4. Verify that the operation has been completed by using the `metrocluster operation show` command.

```
controller_A_1:> metrocluster operation show
  Operation: heal-aggregates
    State: successful
Start Time: 7/25/2016 18:45:55
End Time: 7/25/2016 18:45:56
Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1:> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes      RAID
Status
-----
...
aggr_b2      227.1GB   227.1GB   0% online      0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A:> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

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

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

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.

If your storage system is running ONTAP 9.17.1 or later, use the [automated boot recovery procedure](#). If your system is running an earlier version of ONTAP, you must use the manual boot recovery process.

Step 1: Remove the controller module

To access components inside the controller module, you must remove the controller module from the chassis.

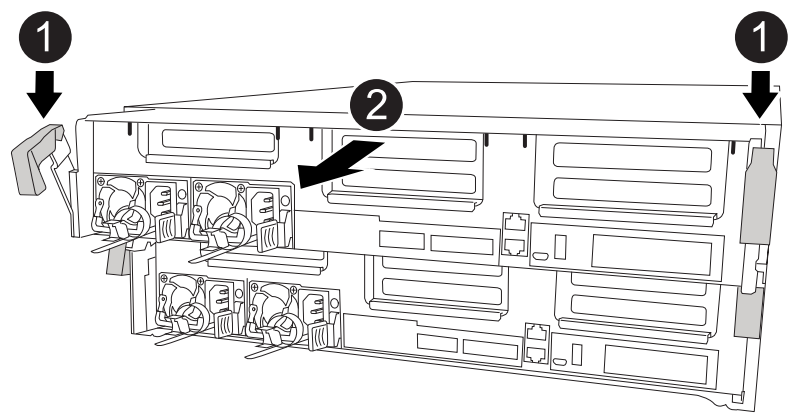
Steps

- 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 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	Controller moves slightly 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.



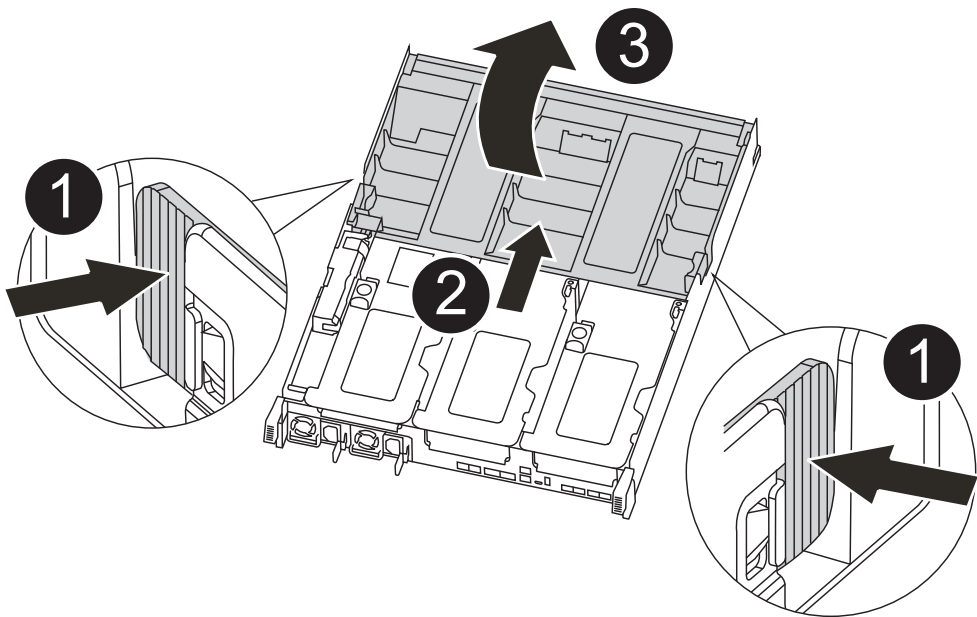
You must log into the NetApp Support Site to display the *Statement of Volatility* for your system.

You can use the following animation, illustration, or the written steps to replace the boot media.

[Animation - Replace the boot media](#)

Steps

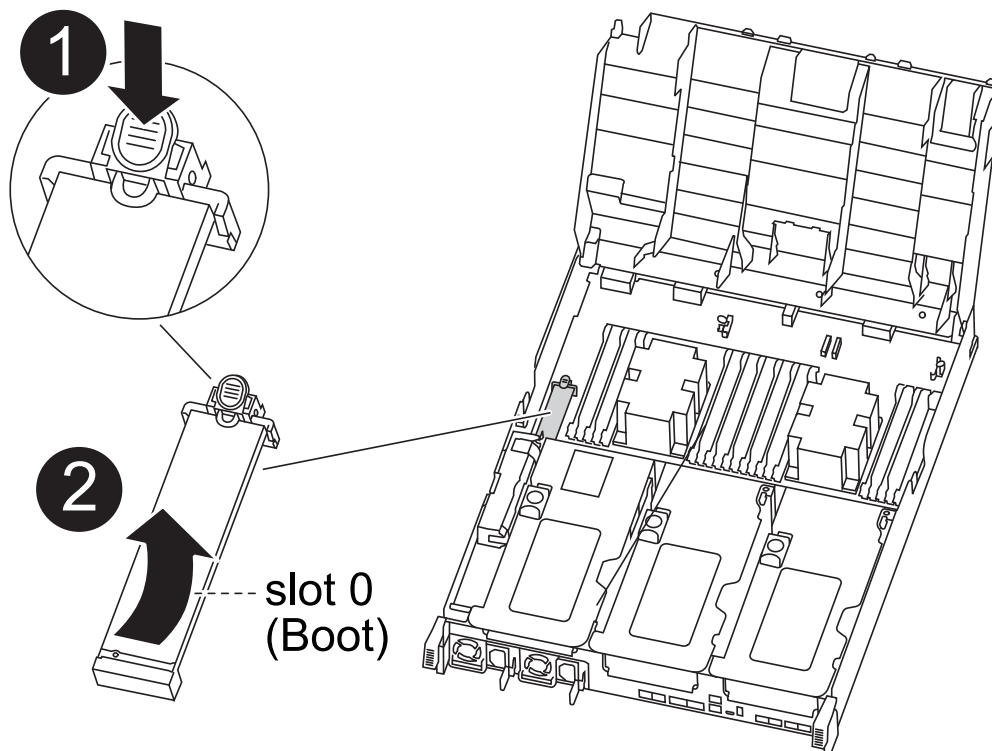
1. Open the air duct:



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 reseal 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.

Steps

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.



If the service image has no `efi` folder, see [EFI folder missing from Service Image download file used for boot device recovery for FAS and AFF models^](#).

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.

Manual boot media recovery from a USB drive - ASA C400

After installing the new boot media device in your system, you can boot the recovery image from a USB drive and restore the configuration from the partner node.

If your storage system is running ONTAP 9.17.1 or later, use the [automated boot recovery procedure](#). If your system is running an earlier version of ONTAP, you must use the manual boot recovery process.

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:

Option 1: ONTAP 9.16.0 or earlier

- a. On the impaired controller, press `Y` when you see `Do you want to restore the backup configuration now?`
- b. If prompted on the impaired controller, press `Y` to overwrite `/etc/ssh/ssh_host_ecdsa_key`.
- c. On the healthy partner controller, set the impaired controller to advanced privilege level: `set -privilege advanced`.
- d. On the healthy partner controller, run the restore backup command: `system node restore-backup -node local -target-address impaired_node_IP_address`.

NOTE: If you see any message other than a successful restore, contact [NetApp Support](#).

- e. On the healthy partner controller, return the impaired controller to admin level: `set -privilege admin`.
- f. On the impaired controller, press `Y` when you see `Was the restore backup procedure successful?`.
- g. On the impaired controller, press `Y` when you see `...would you like to use this restored copy now?`.
- h. On the impaired controller, press `Y` when prompted to reboot the impaired controller and press `ctrl-c` for the Boot Menu.
- i. If the system does not use encryption, select *Option 1 Normal Boot.*, otherwise go to [Restore encryption](#).

Option 2: ONTAP 9.16.1 or later

- a. On the impaired controller, press `Y` when prompted to restore the backup configuration.

After restore procedure is successful, this message will be seen on the console -
`syncflash_partner: Restore from partner complete.`

- b. On the impaired controller, press `Y` when prompted to confirm if the restore backup was successful.
- c. On the impaired controller, press `Y` when prompted to use the restored configuration.
- d. On the impaired controller, press `Y` when prompted to reboot the node.
- e. On the impaired controller, press `Y` when prompted to reboot the impaired controller and press `ctrl-c` for the Boot Menu.
- f. If the system does not use encryption, select *Option 1 Normal Boot.*, otherwise go to [Restore encryption](#).

4. Connect the console cable to the partner controller.
5. Give back the controller using the `storage failover giveback -fromnode local` command.
6. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
7. If AutoSupport is enabled, restore/unsuppress automatic case creation by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.

NOTE: If the process fails, contact [NetApp Support](#).

Restore encryption - ASA C400

Restore encryption on the replacement boot media.

If your storage system is running ONTAP 9.17.1 or later, use the [automated boot recovery procedure](#). If your system is running an earlier version of ONTAP, you must use the manual boot recovery process.

You must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled using the settings that you captured at the beginning of the boot media replace procedure.

Depending on which a key manger is configured on your system, select one of the following options to restore it from the boot menu.

- [Option 1: Restore the Onboard Key Manager configuration](#)
- [Option 2: Restore the External Key Manager configuration](#)

Option 1: Restore the Onboard Key Manager configuration

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

Before you begin

- Make sure you have following information while restoring the OKM configuration:
 - Cluster-wide passphrase entered [while enabling onboard key management](#).
 - [Backup information for the Onboard Key Manager](#).
- Perform the [How to verify onboard key management backup and cluster-wide passphrase](#) procedure before proceeding.

Steps

1. Connect the console cable to the target controller.
2. From the ONTAP boot menu select the appropriate option from the boot menu.

ONTAP version	Select this option
ONTAP 9.8 or later	<p data-bbox="621 153 829 191">Select option 10.</p> <p data-bbox="621 222 948 254">Show example boot menu</p> <div data-bbox="654 296 1456 1081"> <p data-bbox="683 331 1294 363">Please choose one of the following:</p> <ul data-bbox="683 411 1369 1010" style="list-style-type: none"> <li data-bbox="683 411 971 443">(1) Normal Boot. <li data-bbox="683 453 1133 485">(2) Boot without /etc/rc. <li data-bbox="683 495 1045 527">(3) Change password. <li data-bbox="683 537 1369 600">(4) Clean configuration and initialize all disks. <li data-bbox="683 611 1149 642">(5) Maintenance mode boot. <li data-bbox="683 653 1328 684">(6) Update flash from backup config. <li data-bbox="683 695 1240 726">(7) Install new software first. <li data-bbox="683 737 976 768">(8) Reboot node. <li data-bbox="683 779 1192 842">(9) Configure Advanced Drive Partitioning. <li data-bbox="683 852 1333 915">(10) Set Onboard Key Manager recovery secrets. <li data-bbox="683 926 1317 989">(11) Configure node for external key management. <p data-bbox="683 1010 1032 1041">Selection (1-11)? 10</p> </div>

ONTAP version	Select this option
ONTAP 9.7 and earlier	<p>Select the hidden option <code>recover_onboard_keymanager</code></p> <p>Show example boot menu</p> <div> <pre> Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager </pre> </div>

3. Confirm that you want to continue the recovery process.

Show example prompt

```

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

```

4. Enter the cluster-wide passphrase twice.

While entering the passphrase the console will not show any input.

Show example prompt

```

Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:

```

5. Enter the backup information.

a. Paste the entire content from the BEGIN BACKUP line through the END BACKUP line.

Show example prompt

Enter the backup data:

```
-----BEGIN BACKUP-----
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----
```

b. Press the enter key twice at the end of the input.

The recovery process completes.

Show example prompt

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

Successfully recovered keymanager secrets.

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



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

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

Show example prompt

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

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

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

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

8. From the partner node, giveback the partner controller by entering the following command.

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

9. After booting with only the CFO aggregate, run the following command.

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

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

Show example prompt

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

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



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

11. Ensure that all keys are synced by entering the following command.

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

There are no entries matching your query.



No results should appear when filtering for false in the restored parameter.

12. Giveback the node from the partner by entering the following command.

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

13. Restore automatic giveback, if you disabled it, by entering the following command.

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

14. If AutoSupport is enabled, restore automatic case creation by entering the following command.

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

Option 2: Restore the External Key Manager configuration

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

Before you begin

You need the following information for restoring the External Key Manager (EKM) configuration.

- A copy of the /cfcard/kmip/servers.cfg file from another cluster node or the following information:
 - The KMIP server address.
 - The KMIP port.
- A copy of the /cfcard/kmip/certs/client.crt file from another cluster node or the client certificate.

- A copy of the `/cfcard/kmip/certs/client.key` file from another cluster node or the client key.
- A copy of the `/cfcard/kmip/certs/CA.pem` file from another cluster node or the KMIP server CA(s).

Steps

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

Show example boot menu

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

3. When prompted, confirm you have gathered the required information.

Show example prompt

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

4. When prompted, enter the client and server information.

Show prompt

```
Enter the client certificate (client.crt) file contents:
Enter the client key (client.key) file contents:
Enter the KMIP server CA(s) (CA.pem) file contents:
Enter the server configuration (servers.cfg) file contents:
```

Show example

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

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

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

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

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

After you enter the client and server information, the recovery process completes.

Show example

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

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

Show example prompt

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

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

6. Restore automatic giveback if you disabled it.

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

7. If AutoSupport is enabled, restore automatic case creation by entering the following command.

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

Return the failed boot media to NetApp - ASA C400

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

Chassis

Overview of chassis replacement - ASA C400

To replace the chassis, you must move the fans and controller modules from the impaired chassis to 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 disruptive. For a two-node cluster, you will have a complete service outage and a partial outage in a multinode cluster.

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

Option 1: Shut down the controllers when replacing a chassis

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

Before you begin

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

Steps

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

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

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

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

6. Exit the cluster shell:

```
exit
```

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

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

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

```
system node halt -node <node1>,<node2> -skip-lif-migration-before-shutdown
```

```
true -ignore-quorum-warnings true -inhibit-takeover true
```



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

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

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

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

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

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

About this task

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

Steps

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

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

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

```
controller_A_1:> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the `metrocluster operation show` command.

```
controller_A_1::> metrocluster operation show
  Operation: heal-aggregates
    State: successful
Start Time: 7/25/2016 18:45:55
  End Time: 7/25/2016 18:45:56
    Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes      RAID
Status
-----
...
aggr_b2      227.1GB   227.1GB    0% online    0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

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

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

Move the fans, hard drives, and controller module from the impaired chassis to the new chassis, and swap out the impaired chassis 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.

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.

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.
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.

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.

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. 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 - ASA C400

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

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

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

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. Reinstall the bezel on the front of the system.

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

This task only applies to two-node MetroCluster configurations.

Steps

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

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node              State          Mirroring Mode
-----
1      cluster_A
      controller_A_1 configured      enabled    heal roots
completed
      cluster_B
      controller_B_1 configured      enabled    waiting for
switchback recovery
2 entries were displayed.
```

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

The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show

Cluster              Configuration State      Mode
-----
Local: cluster_B configured      switchover
Remote: cluster_A configured      waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show

Cluster              Configuration State      Mode
-----
Local: cluster_B configured      normal
Remote: cluster_A configured      normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 3: Return the failed part to NetApp

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

Controller

Overview of controller module replacement - ASA C400

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 - ASA C400

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

Option 1: Most systems

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

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

Option 2: Controller is in a two-node MetroCluster

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

About this task

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

Steps

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

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

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

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the `metrocluster operation show` command.

```
controller_A_1:> metrocluster operation show
  Operation: heal-aggregates
    State: successful
Start Time: 7/25/2016 18:45:55
  End Time: 7/25/2016 18:45:56
    Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1:> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes
RAID Status
-----
...
aggr_b2      227.1GB   227.1GB    0% online      0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A:> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

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

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

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

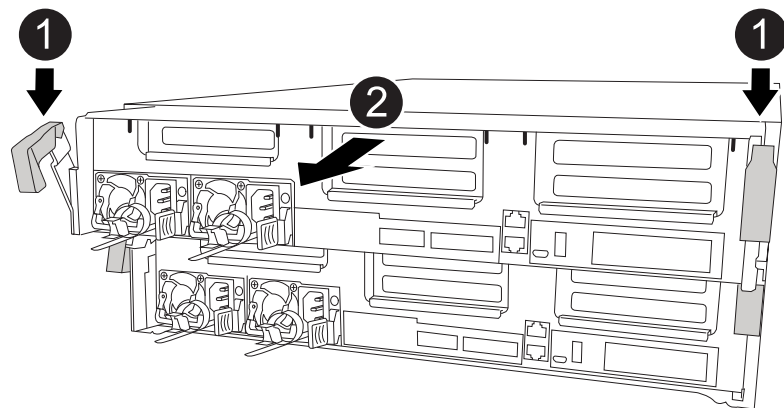
To access components inside the controller module, you must remove the controller module from the chassis.

- 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.



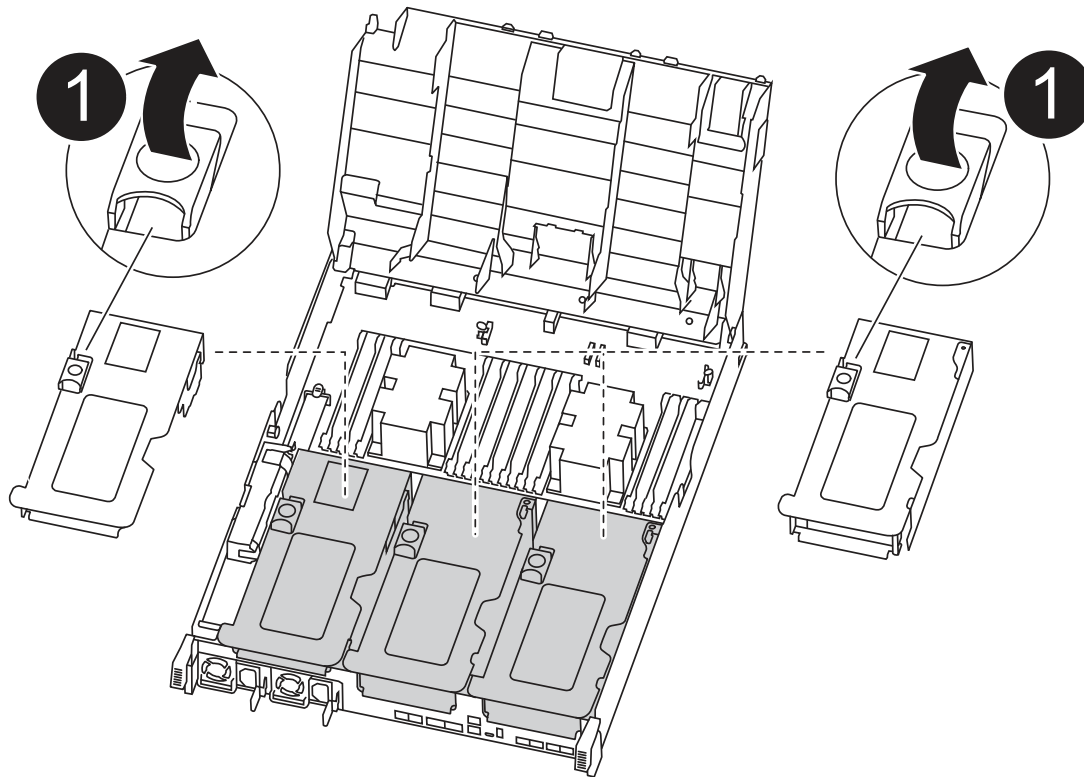
1	Locking latches
2	Controller moves slightly out of chassis

- 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.
- 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:

Animation - Remove the empty risers from the replacement controller module



1

Riser latches

- 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.

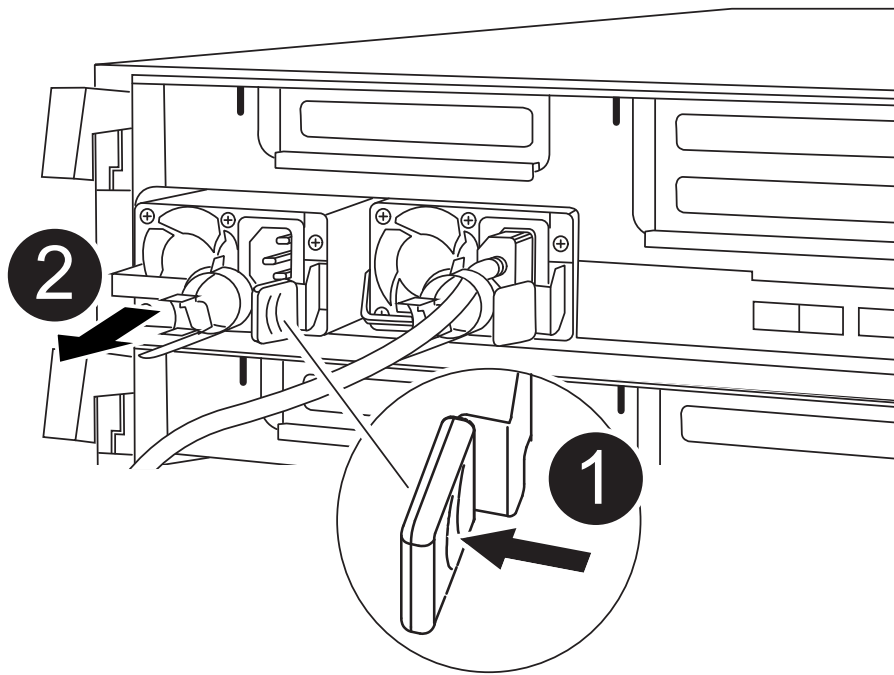
Step 2: Move the power supplies

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.

Animation - Move the power supplies

1. Remove the power supply:



1	PSU locking tab
2	Power cable retainer

- 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.
 1. Move the power supply to the new controller module, and then install it.
 2. 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.



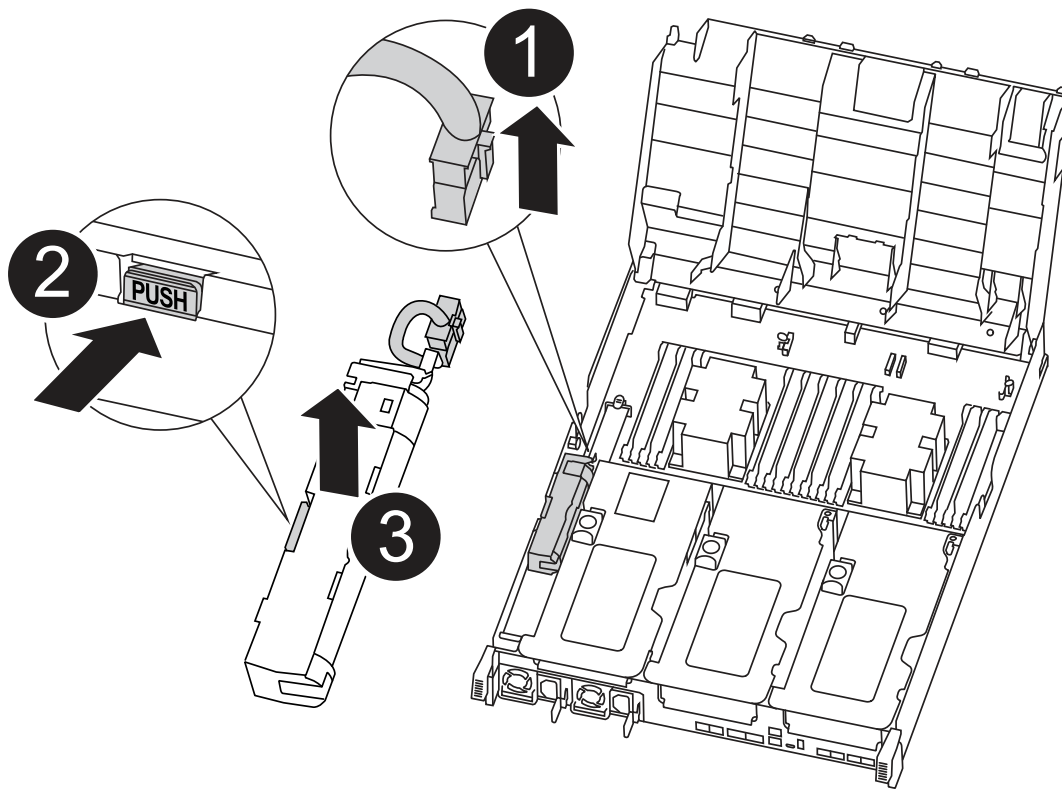
To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

3. 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.



1	NVDIMM battery plug
2	NVDIMM battery locking tab
3	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.
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. Align the battery module with the opening for the battery, and then gently push the battery into slot until it locks into place.



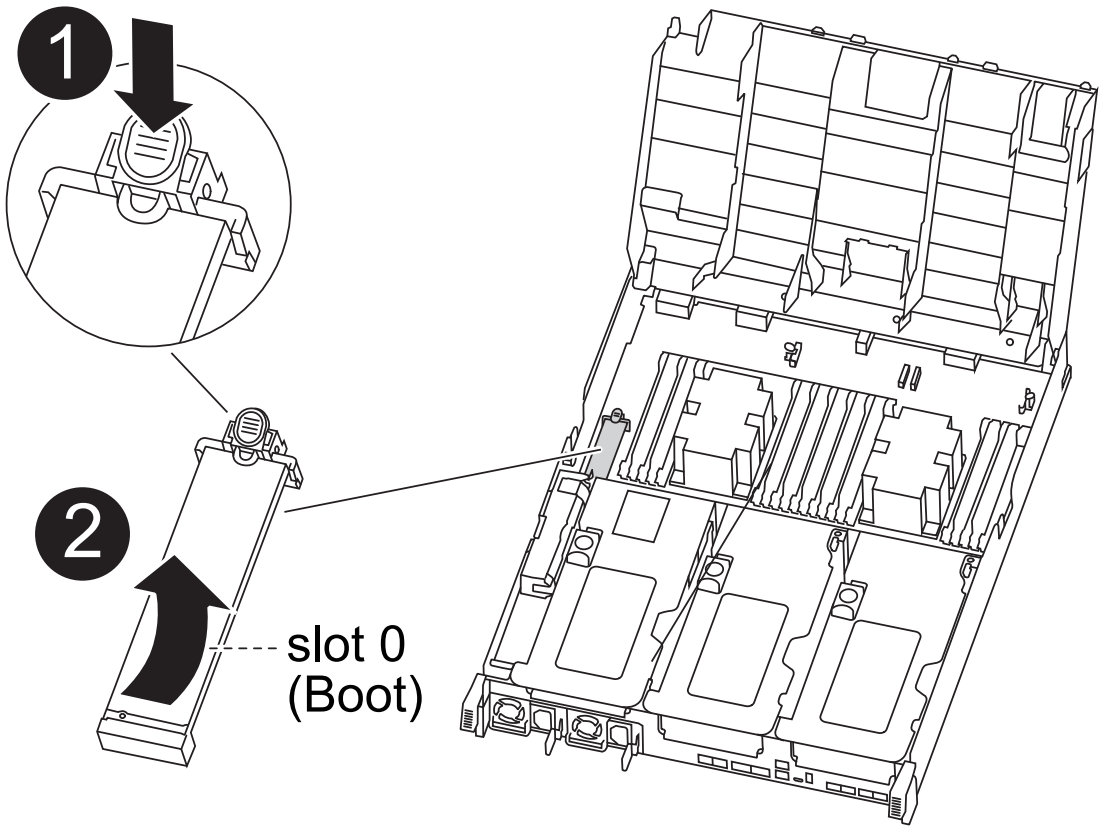
Do not plug the battery cable back into the motherboard until instructed to do so.

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.

Animation - Move the boot media



1	Boot media locking tab
2	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 reseal 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.

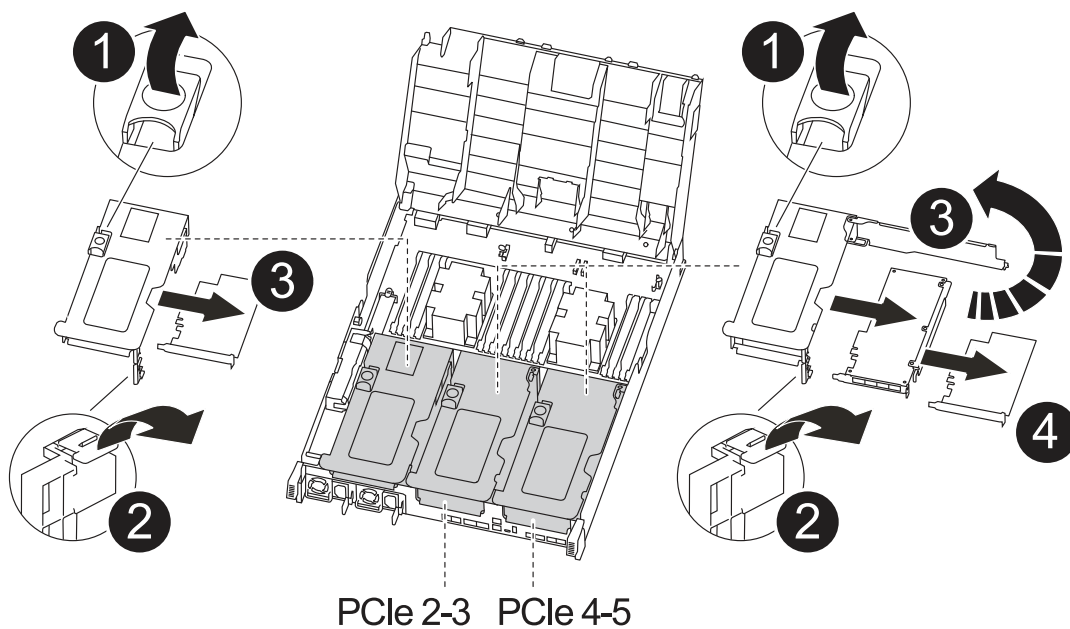
You can use the following animations, illustrations, or the written steps to move the PCIe risers and mezzanine card from the impaired controller module to the replacement controller module.

Moving PCIe riser 1 and 2 (left and middle risers):

[Animation - Move PCI risers 1 and 2](#)

Moving the mezzanine card and riser 3 (right riser):

[Animation - Move the mezzanine card and riser 3](#)



1	Riser locking latch
2	PCI card locking latch
3	PCI locking plate
4	PCI card

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.

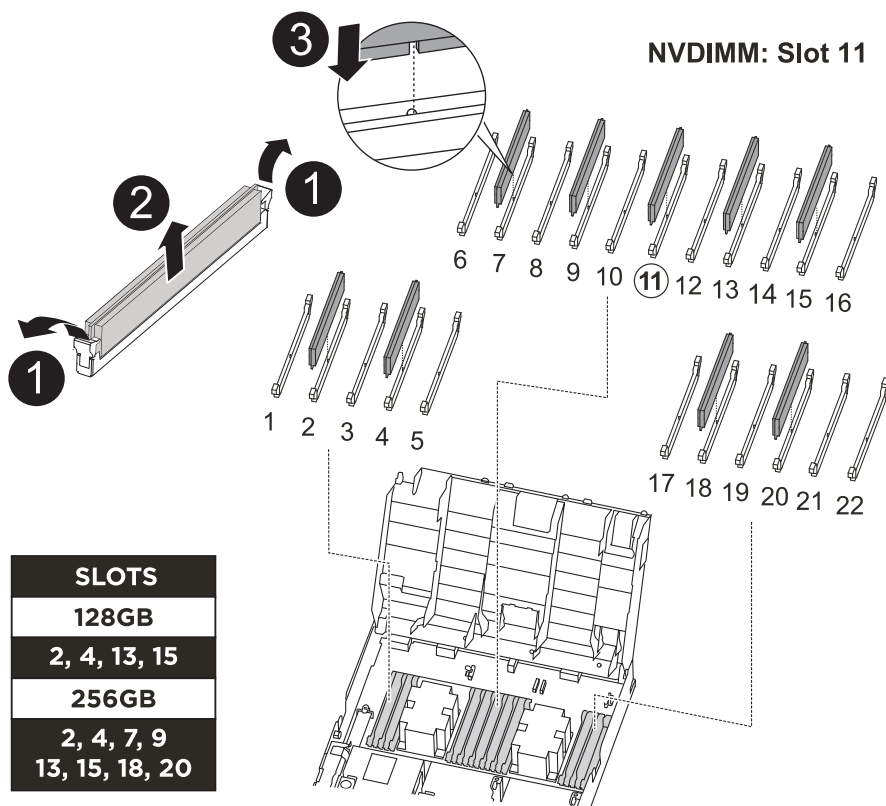
Step 6: Move the DIMMs

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.

[Animation - Move the DIMMs](#)



1	DIMM locking tabs
2	DIMM
3	DIMM socket

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.

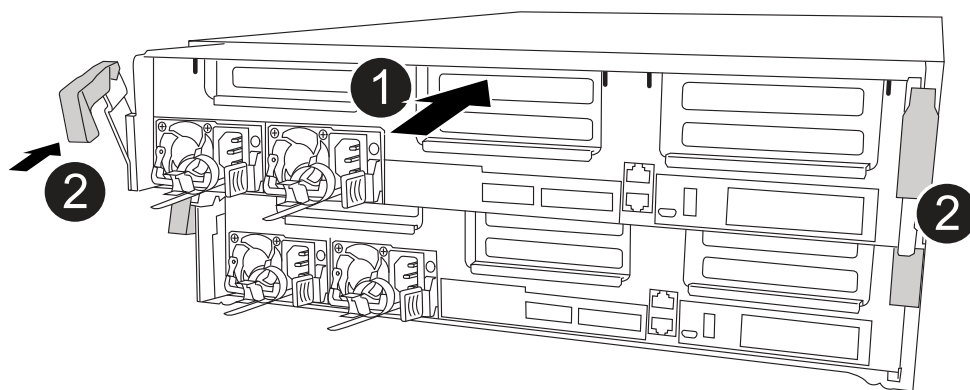
Step 7: Install the controller module

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.

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.



1	Slide controller into the chassis
2	Locking latches

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 - ASA C400

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: `cluster date show`

The date and time are based on the configured timezone.

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

The date and time are given in GMT.

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

The date and time are given in GMT.

Step 2: Verify and set the 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`

Recable the system and reassign disks - ASA C400

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

Step 1: Recable the system

Verify the controller module's storage and network connections.

Steps

1. 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: `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`
```

Node	Partner	Takeover Possible	State Description
-----	-----	-----	

node1	node2	false	System ID changed on partner (Old: 151759706), In takeover
node2	node1	-	Waiting for giveback (HA mailboxes)

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

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

6. Give back the 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.

7. 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
.
.
.
```

8. 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.

9. 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](#)

10. 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.
```

11. Verify that the expected volumes are present for each controller: `vol show -node node-name`
12. 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 - ASA C400

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.



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

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: 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 -vserver * -lif *`

2. Register the system serial number with NetApp Support.
 - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
 - If AutoSupport is not enabled, call [NetApp Support](#) to register the serial number.
3. Check the health of your cluster. See the [How to perform a cluster health check with a script in ONTAP](#) KB article for more information.
4. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.

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

Step 3: Switch back aggregates in a two-node MetroCluster configuration

This task only applies to two-node MetroCluster configurations.

Steps

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

```
cluster_B::> metrocluster node show
```

DR	Configuration	DR
Group Cluster Node	State	Mirroring Mode
1	cluster_A	
	controller_A_1 configured	enabled heal roots
completed	cluster_B	
	controller_B_1 configured	enabled waiting for
	switchback recovery	

2 entries were displayed.

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

The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
```

Cluster	Configuration	State	Mode
Local: cluster_B	configured		switchover
Remote: cluster_A	configured		waiting-for-switchback

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster           Configuration State      Mode
-----
Local: cluster_B configured          normal
Remote: cluster_A configured          normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 4: Return the failed part to NetApp

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

Replace a DIMM - ASA C400

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

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

Option 1: Most configurations

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

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

Option 2: Controller is in a two-node MetroCluster

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

About this task

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

Steps

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

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

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

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the `metrocluster operation show` command.

```
controller_A_1::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: 7/25/2016 18:45:55
End Time: 7/25/2016 18:45:56
Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes
RAID Status
-----
...
aggr_b2        227.1GB    227.1GB    0% online      0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

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

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

Step 2: Remove the controller module

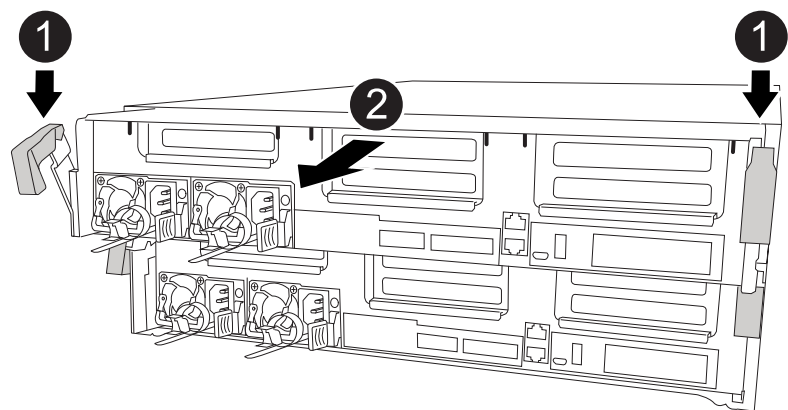
To access components inside the controller module, you must remove the controller module from the chassis.

- 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	Controller moves slightly 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.

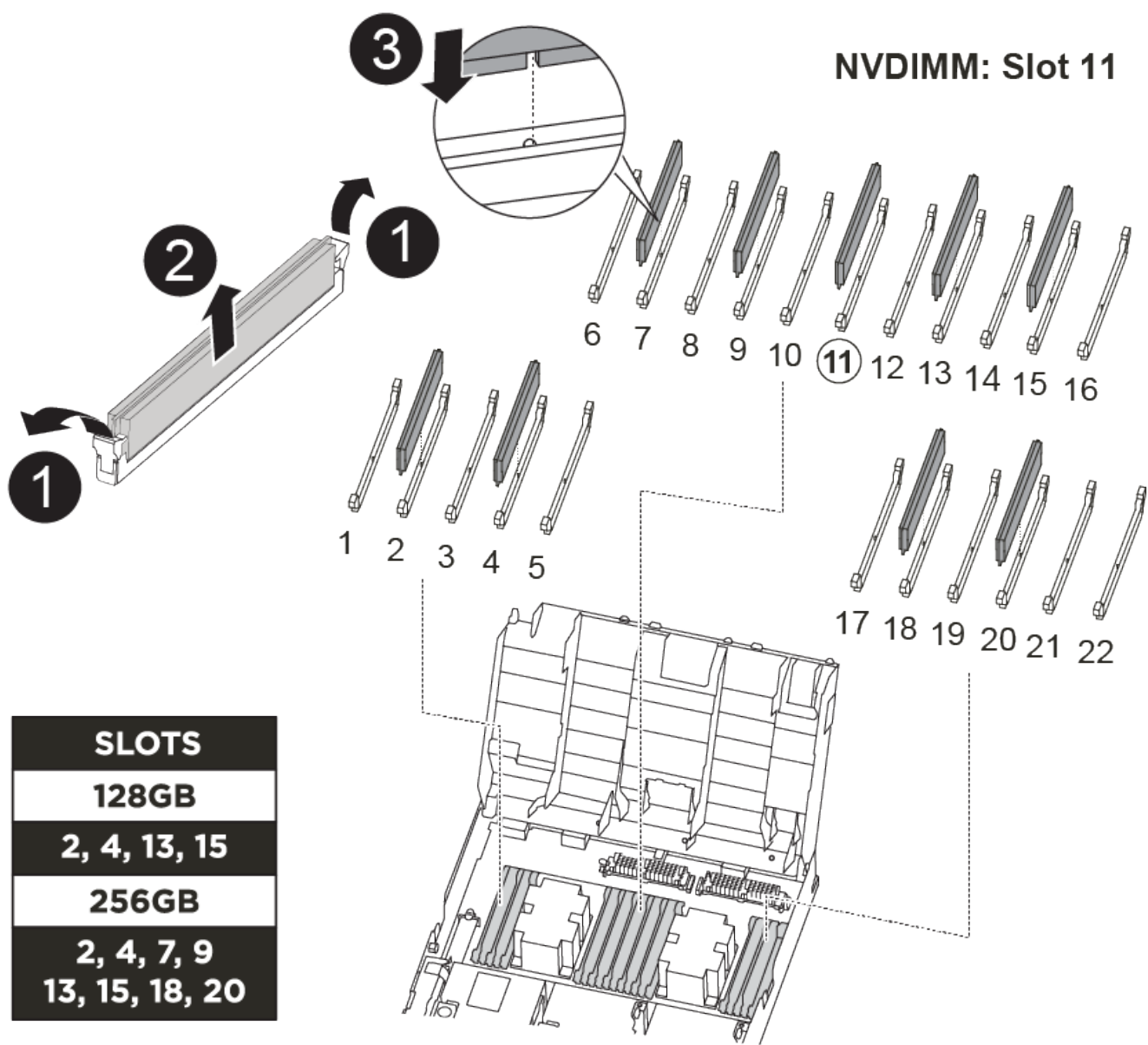
Step 3: Replace system DIMMs

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, 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 show empty slots for sockets without DIMMs. These empty sockets are populated with blanks.



1	DIMM locking tabs
2	DIMM
3	DIMM socket

The DIMMs are located in sockets 2, 4, 13, and 15. The NVDIMM is located in slot 11.

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.

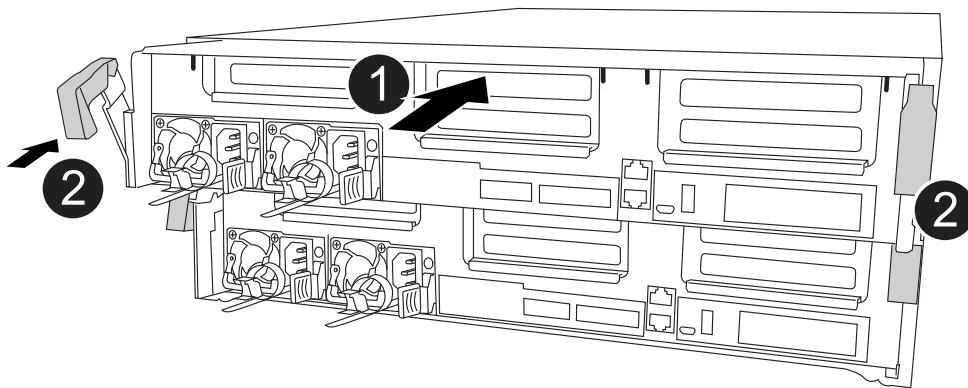


Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

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.



1	Controller module
2	Controller locking latches

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: Restore the controller module to operation

You must recable the system, give back the controller module, and then reen able automatic giveback.

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, reen able it: `storage failover modify -node local -auto`

```
-giveback true
```

Step 6: Switch back aggregates in a two-node MetroCluster configuration

This task only applies to two-node MetroCluster configurations.

Steps

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

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node              State          Mirroring Mode
-----
1      cluster_A
      controller_A_1 configured      enabled      heal roots
completed
      cluster_B
      controller_B_1 configured      enabled      waiting for
switchback recovery
2 entries were displayed.
```

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

The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show

Cluster              Configuration State      Mode
-----
Local: cluster_B configured      switchover
Remote: cluster_A configured      waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster           Configuration State      Mode
-----
Local: cluster_B configured          normal
Remote: cluster_A configured          normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 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 and Replacements](#) page for further information.

Hot-swap a fan module - ASA C400

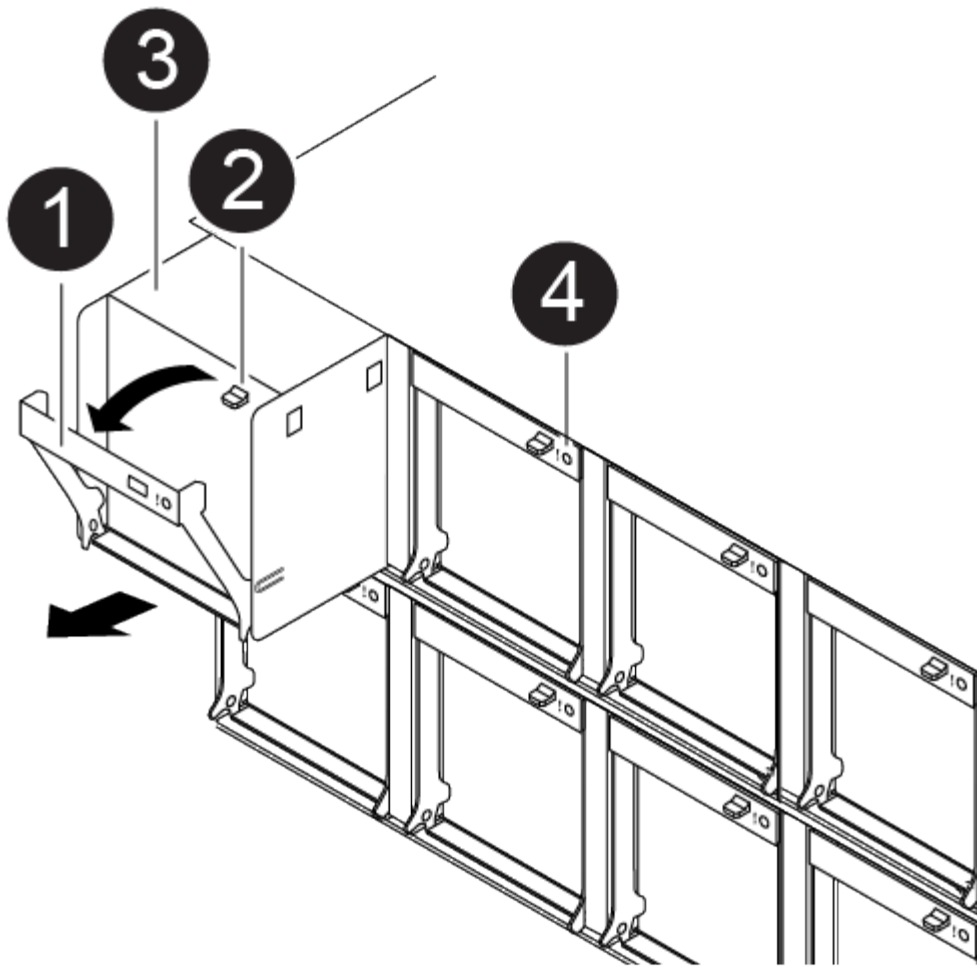
To swap out a fan module without interrupting service, you must perform a specific sequence of tasks.



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.

[Animation - Replace a fan](#)



1	Fan handle
2	Locking tab
3	Fan
4	Status LED

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 and Replacements](#) page for further information.

Replace the NVDIMM battery - ASA C400

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

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

Option 2: Controller is in a two-node MetroCluster

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

About this task

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

Steps

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

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

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

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the `metrocluster operation show` command.

```
controller_A_1::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: 7/25/2016 18:45:55
End Time: 7/25/2016 18:45:56
Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes
RAID Status
-----
...
aggr_b2        227.1GB    227.1GB    0% online      0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

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

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

Step 2: Remove the controller module

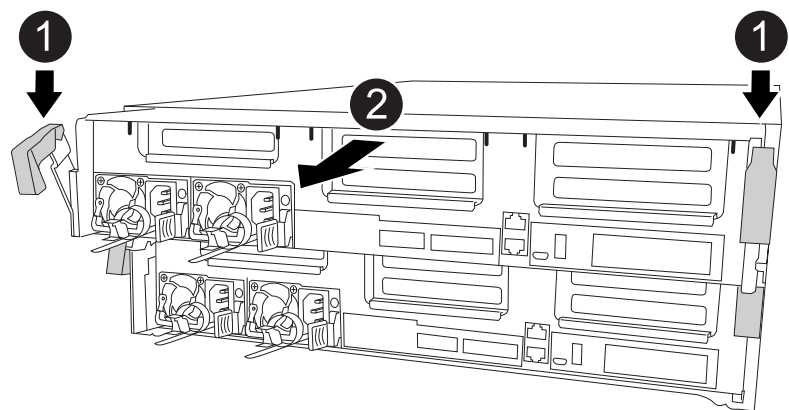
To access components inside the controller module, you must remove the controller module from the chassis.

- 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	Controller moves slightly 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.

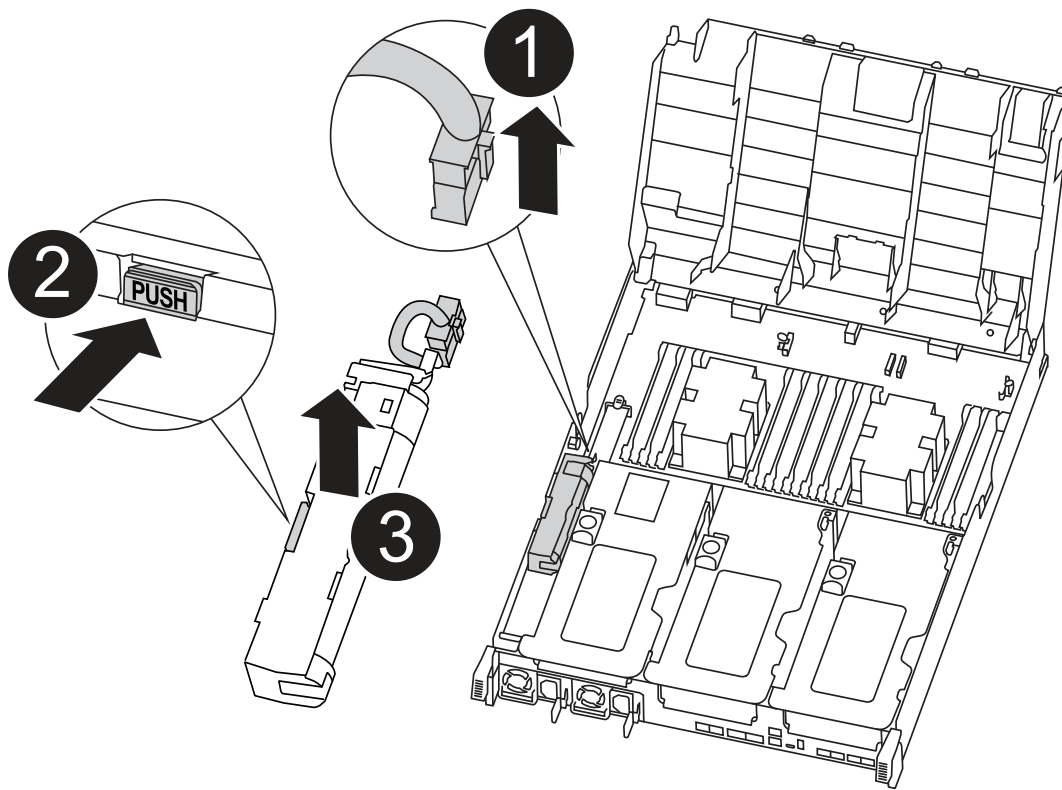
- 7. Place the controller module on a stable, flat surface.

Step 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.

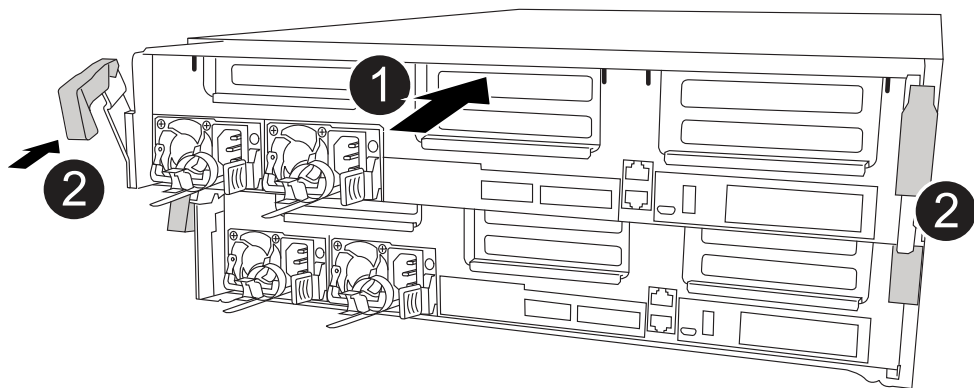


1	Battery plug
2	Locking tab
3	NVDIMM battery

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.
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.



1	Controller module
2	Controller locking latches

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: Restore the controller module to operation

You must recable the system, give back the controller module, and then reenabling automatic giveback.

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, reenabling it: `storage failover modify -node local -auto-giveback true`

Step 6: Switch back aggregates in a two-node MetroCluster configuration

This task only applies to two-node MetroCluster configurations.

Steps

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

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node              State          Mirroring Mode
-----
1      cluster_A
      controller_A_1 configured    enabled    heal roots
completed
      cluster_B
      controller_B_1 configured    enabled    waiting for
switchback recovery
2 entries were displayed.
```

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

The switchback operation is still running when a cluster is in the `waiting-for-switchback` state:

```
cluster_B::> metrocluster show
Cluster              Configuration State      Mode
-----
Local: cluster_B configured          switchover
Remote: cluster_A configured          waiting-for-switchback
```

The switchback operation is complete when the clusters are in the `normal` state.:

```
cluster_B::> metrocluster show
Cluster              Configuration State      Mode
-----
Local: cluster_B configured          normal
Remote: cluster_A configured          normal
```

If a switchback is taking a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command.

6. Reestablish any SnapMirror or SnapVault configurations.

Step 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 and Replacements](#) page for further information.

Replace an NVDIMM - ASA C400

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

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

Option 1: Most configurations

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

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

Option 2: Controller is in a two-node MetroCluster

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

About this task

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

Steps

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

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

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

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the `metrocluster operation show` command.

```
controller_A_1::> metrocluster operation show
  Operation: heal-aggregates
    State: successful
Start Time: 7/25/2016 18:45:55
  End Time: 7/25/2016 18:45:56
    Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes
RAID Status
-----
...
aggr_b2       227.1GB   227.1GB    0% online      0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

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

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

Step 2: Remove the controller module

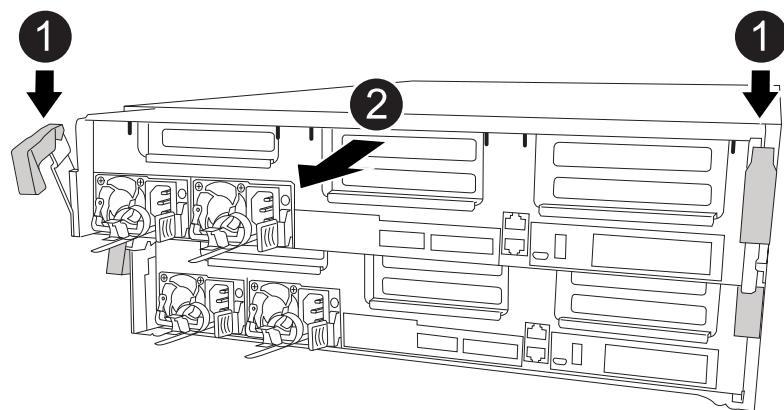
To access components inside the controller module, you must remove the controller module from the chassis.

- 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	Controller moves slightly 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 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 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.



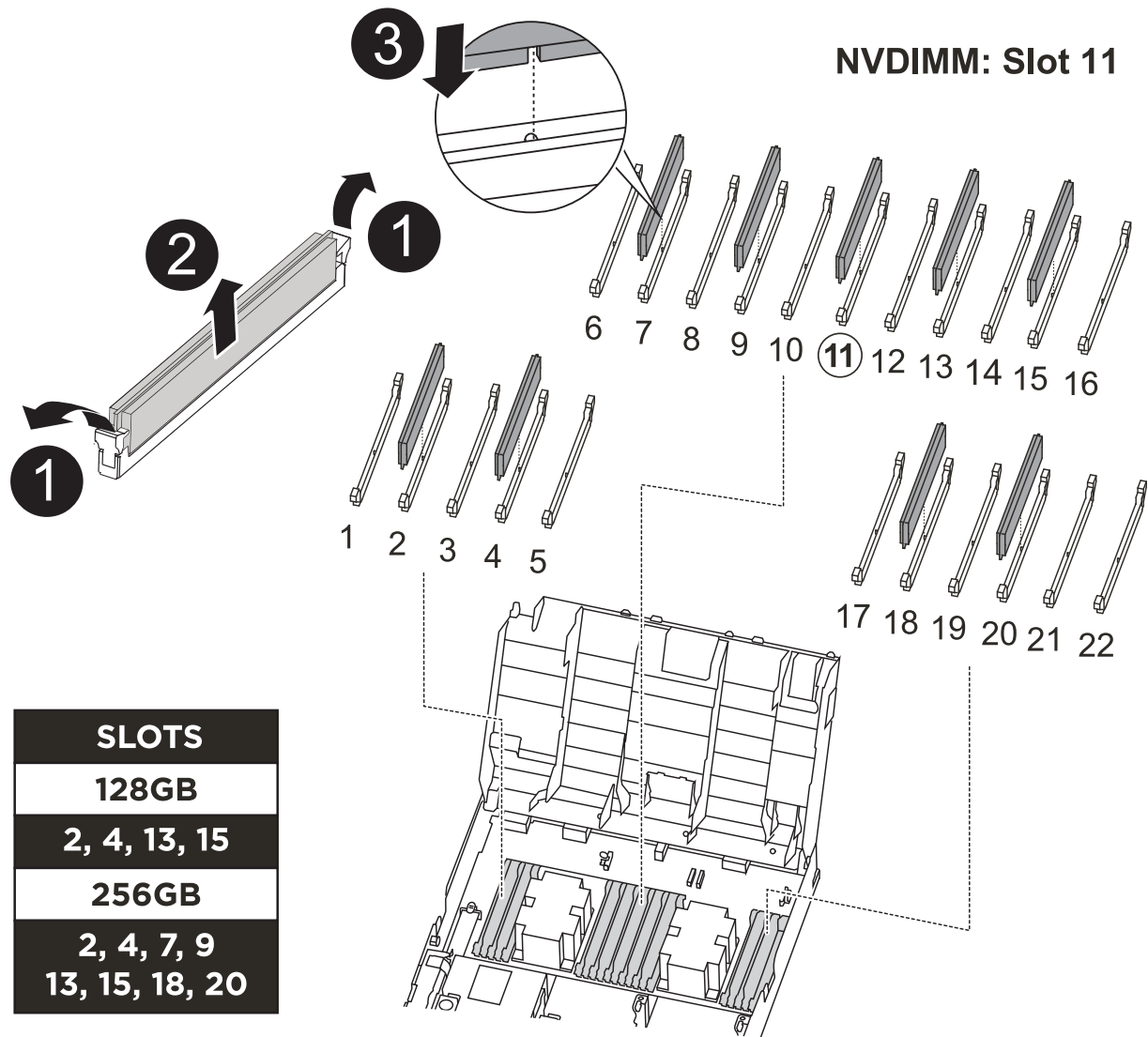
You must log into the NetApp Support Site to display the *Statement of Volatility* for your system.

You can use the following animation, illustration, or the written steps to replace the NVDIMM.



The animation shows empty slots for sockets without DIMMs. These empty sockets are populated with blanks.

Animation - Replace the NVDIMM



1	DIMM locking tabs
2	DIMM

3

DIMM socket

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.

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: Restore the controller module to operation

You must recable the system, give back the controller module, and then reenabling automatic giveback.

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, reenabling it: `storage failover modify -node local -auto-giveback true`

Step 6: Switch back aggregates in a two-node MetroCluster configuration

This task only applies to two-node MetroCluster configurations.

Steps

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

```
cluster_B::> metrocluster node show
```

DR		Configuration	DR
Group	Cluster Node	State	Mirroring Mode
-----	-----	-----	-----
1	cluster_A		
	controller_A_1	configured	enabled
completed	cluster_B		
	controller_B_1	configured	enabled
	switchback recovery		waiting for
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 and Replacements](#) page for further information.

Replace a PCIe or mezzanine card - ASA C400

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

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

Option 2: Controller is in a two-node MetroCluster

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

About this task

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

Steps

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

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

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

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft

vetoos 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-vetoos` parameter. If you use this optional parameter, the system overrides any soft vetoos 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

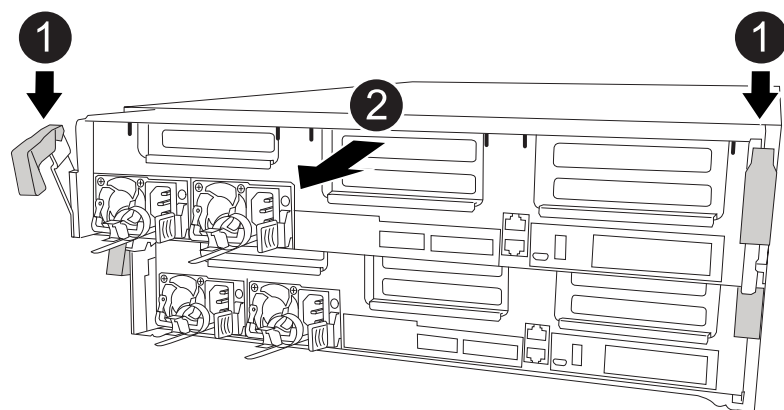
To access components inside the controller module, you must remove the controller module from the chassis.

- 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	Controller moves slightly out of chassis

- 6. Slide the controller module out of the chassis.

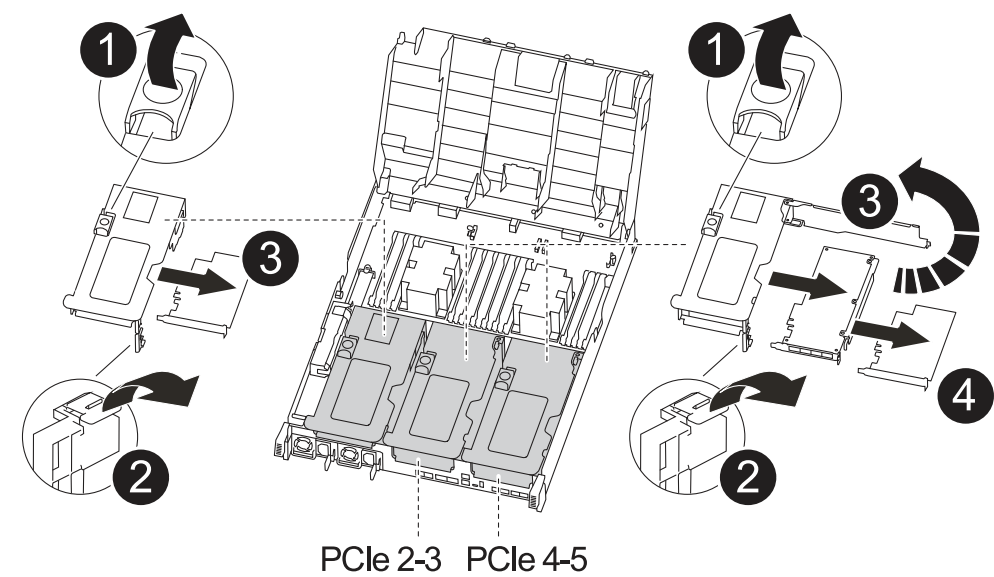
Make sure that you support the bottom of the controller module as you slide it out of the chassis.

- 7. Place the controller module on a stable, flat surface.

Step 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.



1	Riser locking latch
2	PCI card locking latch
3	PCI locking plate
4	PCI card

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:

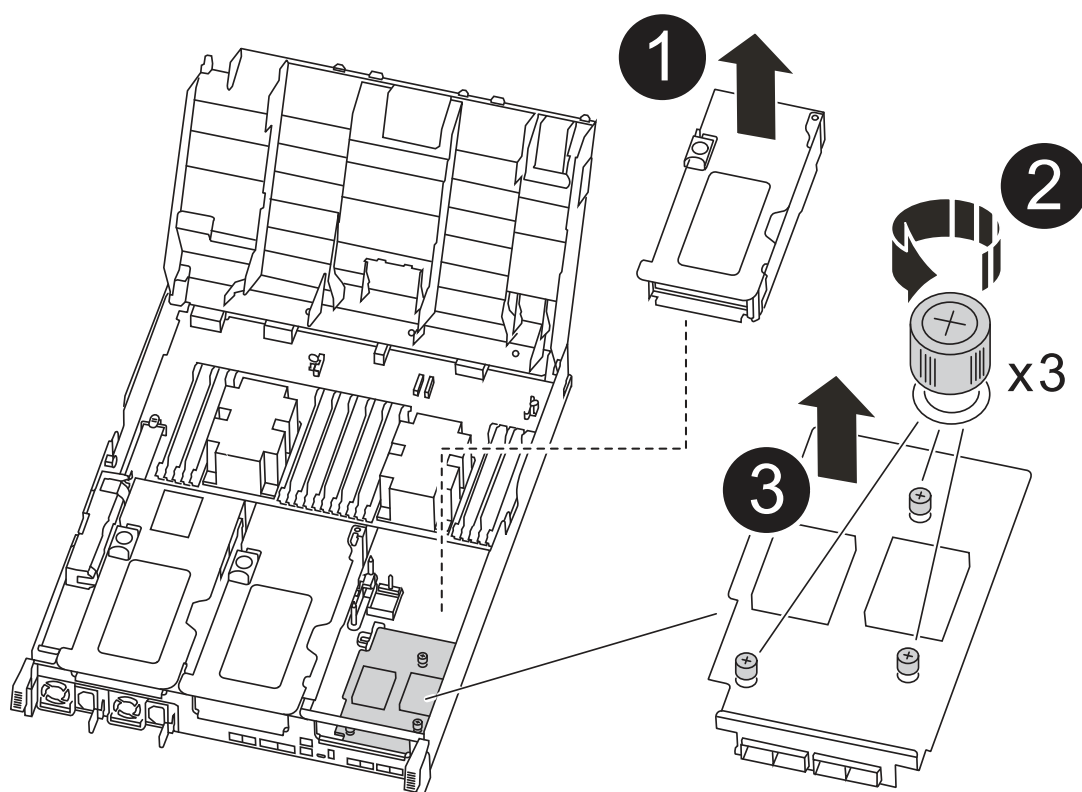
- a. Align the riser with the pins to the side of the riser socket, lower the riser down on the pins.
- b. Push the riser squarely into the socket on the motherboard.
- c. Rotate the latch down flush with the sheet metal on the riser.

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.

[Animation - Replace the mezzanine card](#)



1	PCI riser
---	-----------

2	Riser thumbscrew
3	Riser card

1. Remove riser number 3 (slots 4 and 5):

- 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.
- Remove any SFP or QSFP modules that might be in the PCIe cards.
- 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.

- Lift the riser up, and then set it aside on a stable, flat surface.

2. Replace the mezzanine card:

- Remove any QSFP or SFP modules from the card.
- Loosen the thumbscrews on the mezzanine card, and gently lift the card directly out of the socket and set it aside.
- Align the replacement mezzanine card over the socket and the guide pins and gently push the card into the socket.
- Tighten the thumbscrews on the mezzanine card.

3. Reinstall the riser:

- 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.
- 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.

- If you have not already done so, close the air duct.
- 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:

- 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: Restore the controller module to operation

To restore the controller, you must recable the system, give back the controller module, and then reenable automatic giveback.

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

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 and Replacements](#) page for further information.

Replacing a power supply - ASA C400

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.

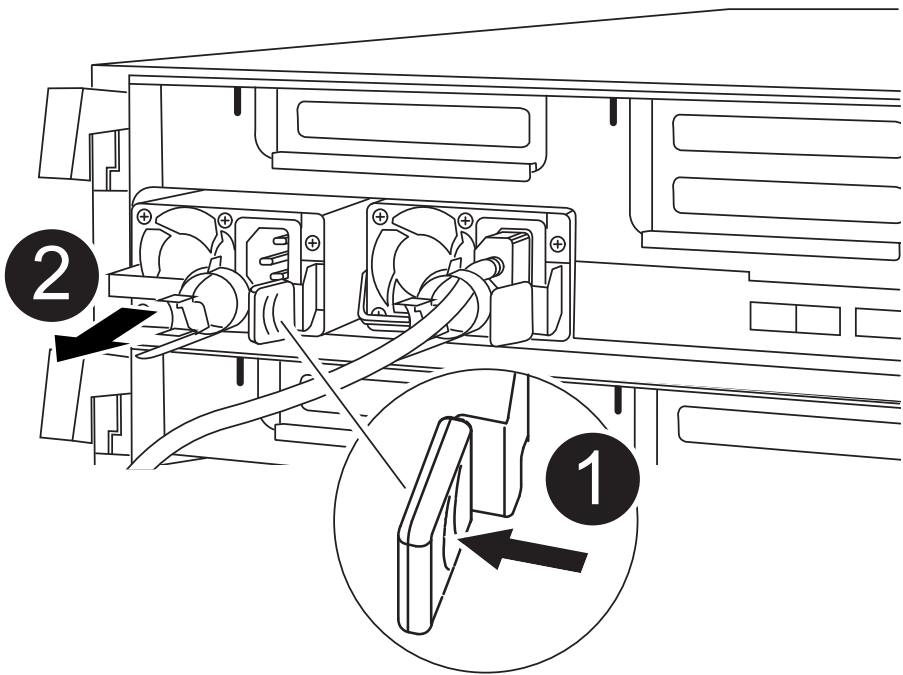


It is a best practice to replace the power supply within two minutes of removing it from the chassis. The system continues to function, but ONTAP sends messages to the console about the degraded power supply until the power supply is replaced.



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

You can use the following illustration with the written steps to replace the power supply.



1	PSU locking tab
2	Power cable retainer

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 and Replacements](#) page for further information.

Replace the real-time clock battery - ASA C400

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

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

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

Option 2: Controller is in a two-node MetroCluster

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

About this task

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

Steps

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

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

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

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Verify that the operation has been completed by using the `metrocluster operation show` command.

```
controller_A_1:> metrocluster operation show
  Operation: heal-aggregates
    State: successful
Start Time: 7/25/2016 18:45:55
  End Time: 7/25/2016 18:45:56
    Errors: -
```

5. Check the state of the aggregates by using the `storage aggregate show` command.

```
controller_A_1:> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes
RAID Status
-----
...
aggr_b2        227.1GB    227.1GB    0% online      0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Heal the root aggregates by using the `metrocluster heal -phase root-aggregates` command.

```
mcc1A:> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `-override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

7. Verify that the heal operation is complete by using the `metrocluster operation show` command on the destination cluster:

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

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

Step 2: Remove the controller module

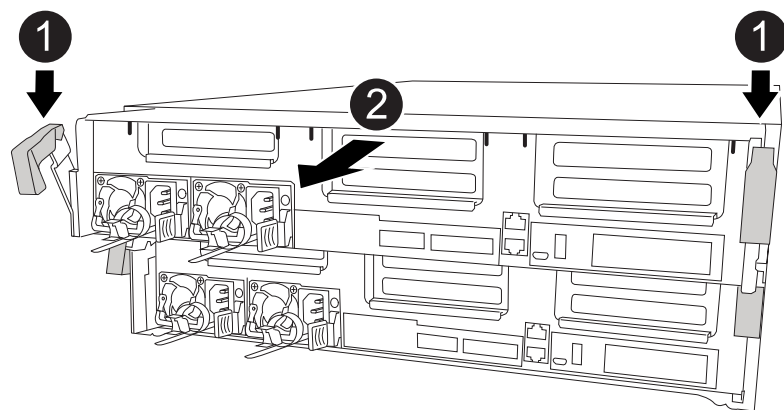
To access components inside the controller module, you must remove the controller module from the chassis.

- 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	Controller moves slightly 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.

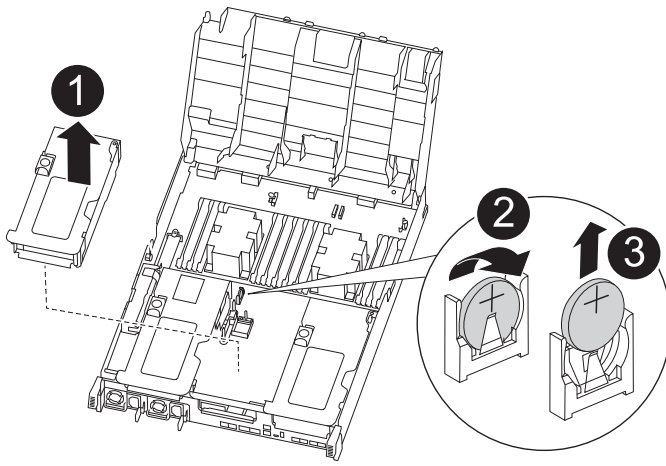
- 7. Place the controller module on a stable, flat surface.

Step 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.

[Animation- Replace the RTC battery](#)



1	Middle riser
2	Remove RTC battery
3	Seat RTC battery

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 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 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

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 and Replacements](#) page for further information.

ASA C800 systems

Install and setup

Start here: Choose your installation and setup experience

For most configurations (including ASA 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 - ASA C800

Quick start gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up.

Use the [ASA C800 Installation and Setup Instructions](#) if you are familiar with installing NetApp systems.

Videos - ASA C800

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.

["Animation - Installation and Setup of an ASA C800"](#)

Video two of two: Perform end-to-end software configuration

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

 | <https://img.youtube.com/vi/Q6orVMYj94A?/maxresdefault.jpg>

Detailed steps - ASA C800

This section gives detailed step-by-step instructions for installing an ASA C800 system.

Step 1: Prepare for installation

To install your ASA C800 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
 - 4U in an HA configuration for the platform
 - 2U for each NS224 storage shelf
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser
 1. Unpack the contents of all boxes.
 2. Record the system serial number from the controllers.



Steps

1. Set up your account:
 - a. Log in to your existing account or create an account.
 - b. Register ([NetApp Product Registration](#)) your system.
2. Download and install [NetApp Downloads: Config Advisor](#) on your laptop.
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 [NetApp Hardware Universe](#) to locate the cable and identify its use.

Connector type	Part number and length	Type of cable...	For...
100 GbE cable	X66211A-05 (112-00595), 0.5m X66211-1 (112-00573), 1m X66211-2 (112-00574), 2m X66211-5 (112-00576), 5m		<ul style="list-style-type: none"> • HA interconnect • Cluster interconnect network • Storage, Data
10 GbE cable	X6566B-3-R6 (112-00300), 3m; X6566B-5-R6 (112-00301), 5m		<ul style="list-style-type: none"> • Data
25 GbE cable	X66240A-2 (112-00598), 2m; X66240A-5 (112-00600), 5m		<ul style="list-style-type: none"> • Data
RJ-45 (order dependent)	Not applicable		<ul style="list-style-type: none"> • Management
Fibre Channel	X66250-2 (112-00342) 2m; X66250-5 (112-00344) 5m; X66250-15 (112-00346) 15m; X66250-30 (112-00347) 30m		<ul style="list-style-type: none"> • Network
Micro-USB console cable	Not applicable		<ul style="list-style-type: none"> • Console connection during software setup
Power cables	Not applicable		Connecting the PSUs to power source

4. Download and complete the [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.

[Installing SuperRail into a four-post rack](#)

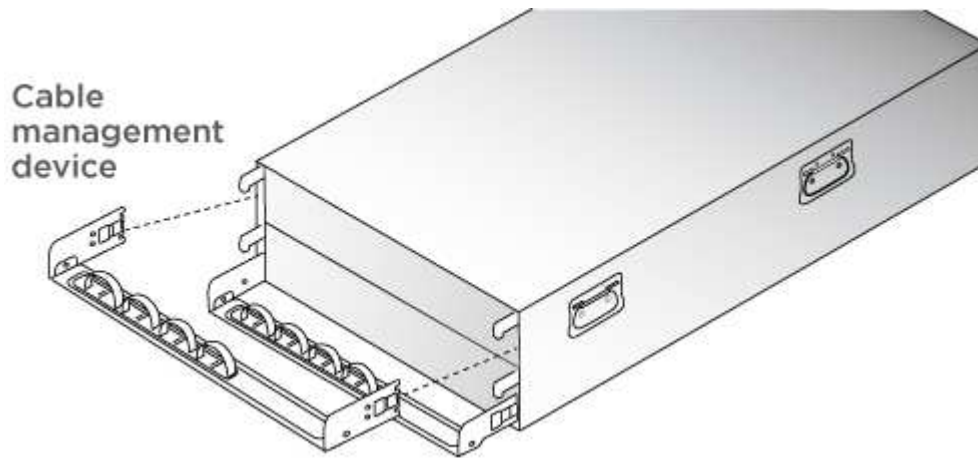
2. Install and secure your system using the instructions included with the rail kit.



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

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.

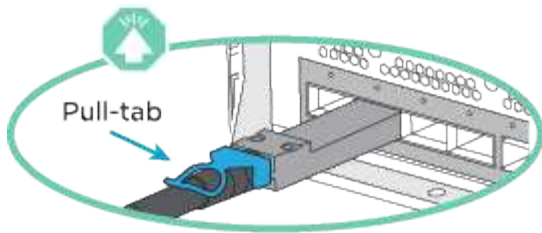
Option 1: Cable a two-node switchless cluster

Management network ports on the controllers are connected to switches. The HA interconnect and cluster interconnect ports are cabled on both controllers.

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.


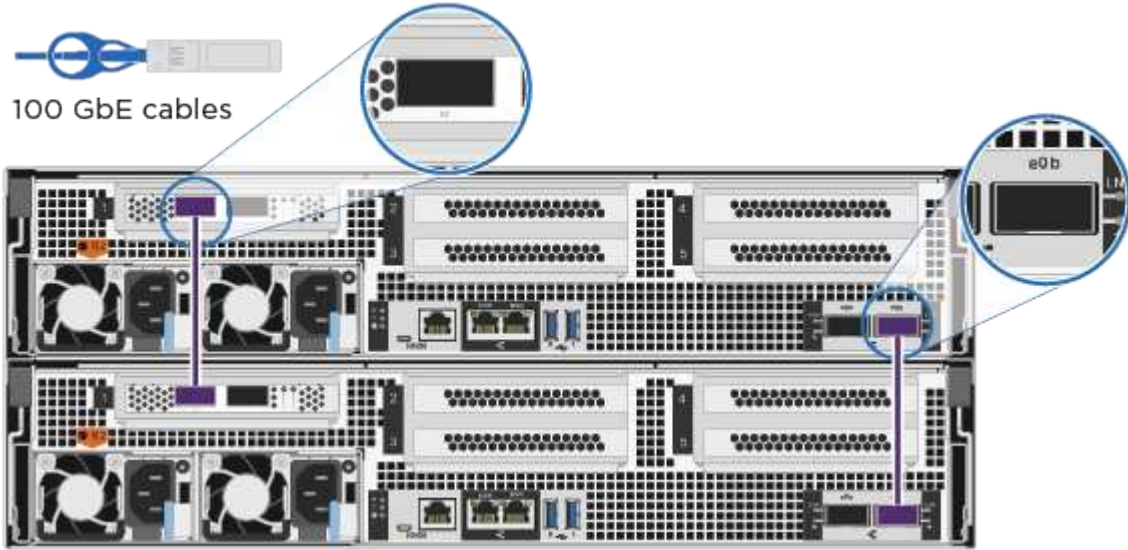


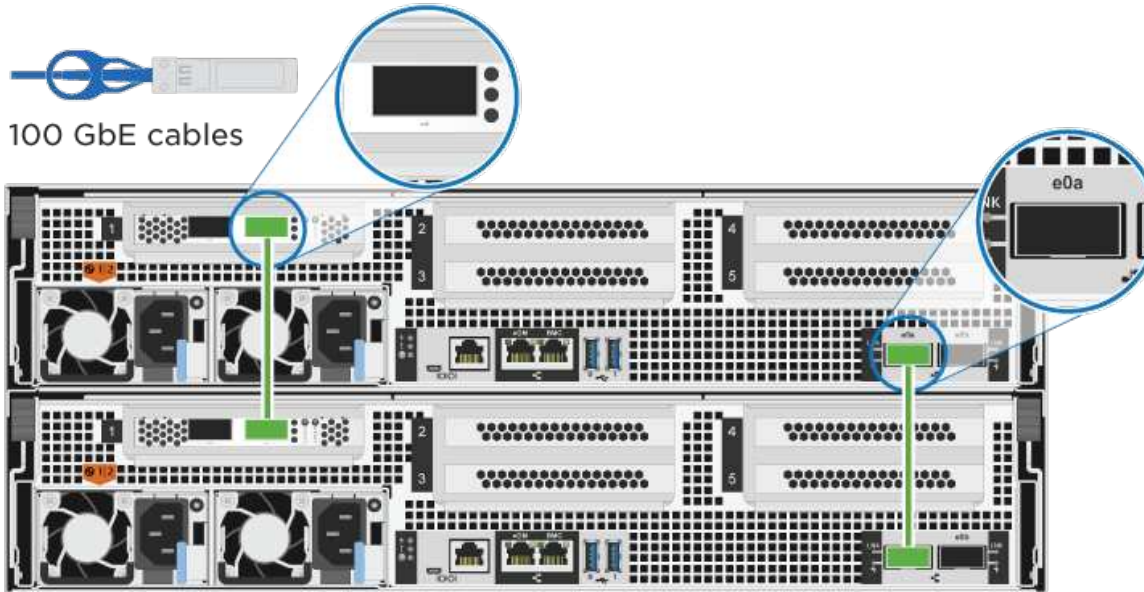
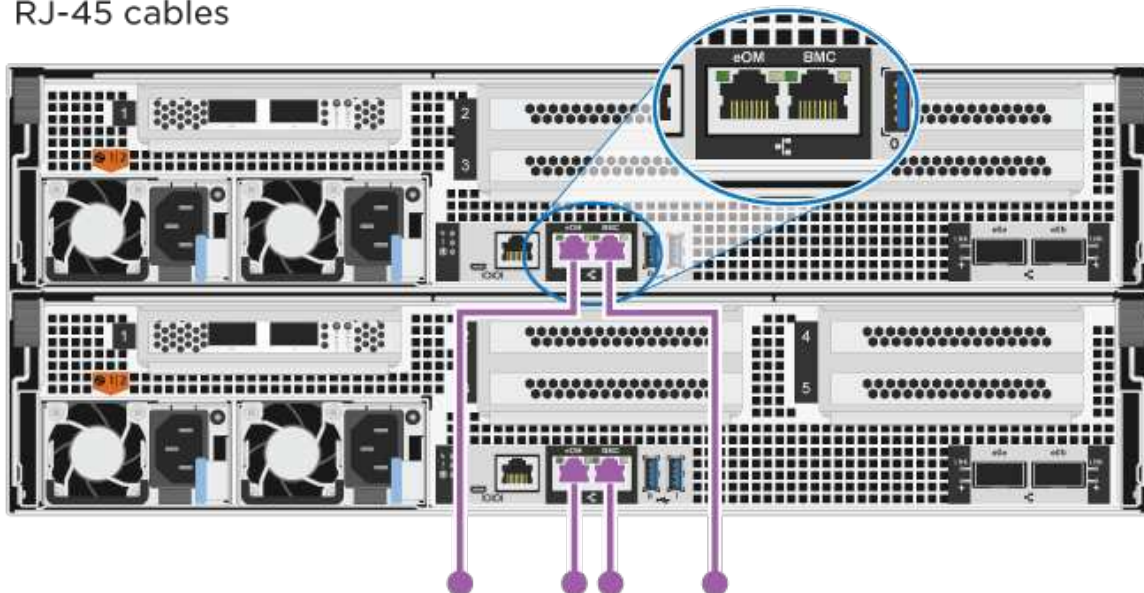

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation or the tabulated steps to complete the cabling between the controllers and the switches:

Animation - Cable a two-node switchless cluster

Step	Perform on each controller module
1	<p>Cable the HA interconnect ports:</p> <ul style="list-style-type: none"> • e0b to e0b • e1b to e1b <p>  100 GbE cables </p> 

Step	Perform on each controller module
2	<p>Cable the cluster interconnect ports:</p> <ul style="list-style-type: none"> • e0a to e0a • e1a to e1a  <p>100 GbE cables</p>
3	<p>Cable the management ports to the management network switches</p>  <p>RJ-45 cables</p>
	DO NOT plug in the power cords at this point.

2. To perform optional cabling, see:

- [Option 1: Cable to a Fibre Channel host network](#)
- [Option 2: Cable to a 10GbE host network](#)
- [Option 3: Cable the controllers to a single drive shelf](#)
- [Option 4: Cable the controllers to two drive shelves](#)

3. To complete setting up your system, see [Step 4: Complete system setup and configuration](#).

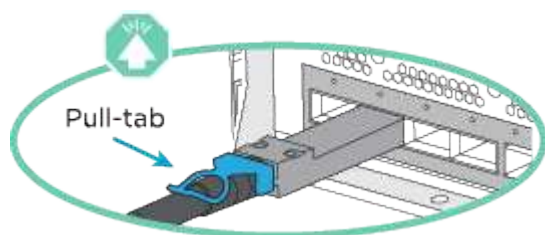
Option 2: Cable a switched cluster

Cluster interconnect and management network ports on the controllers are connected to switches while the HA interconnect ports are cabled on both controllers.

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.

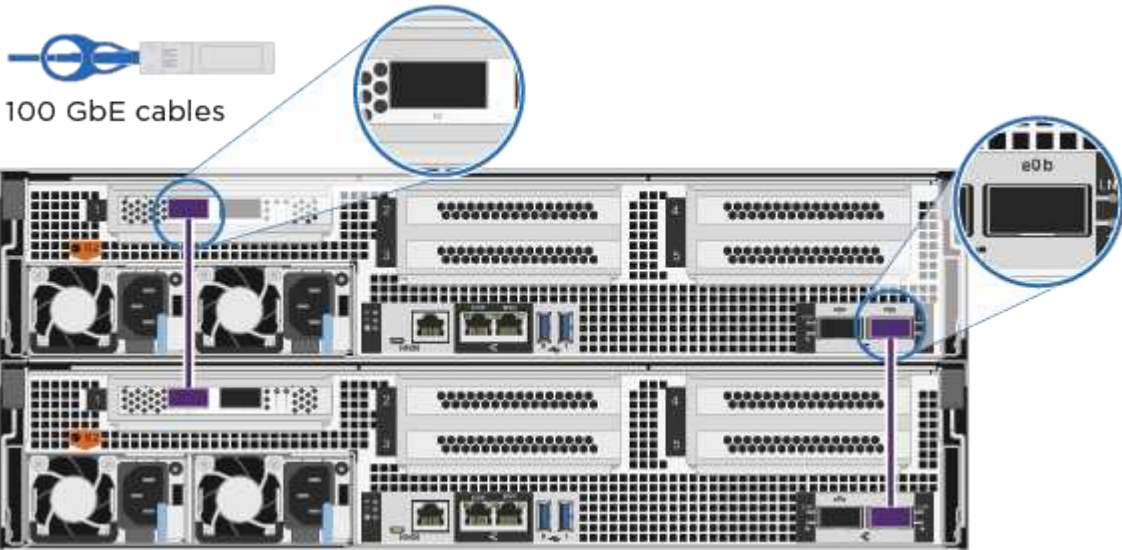
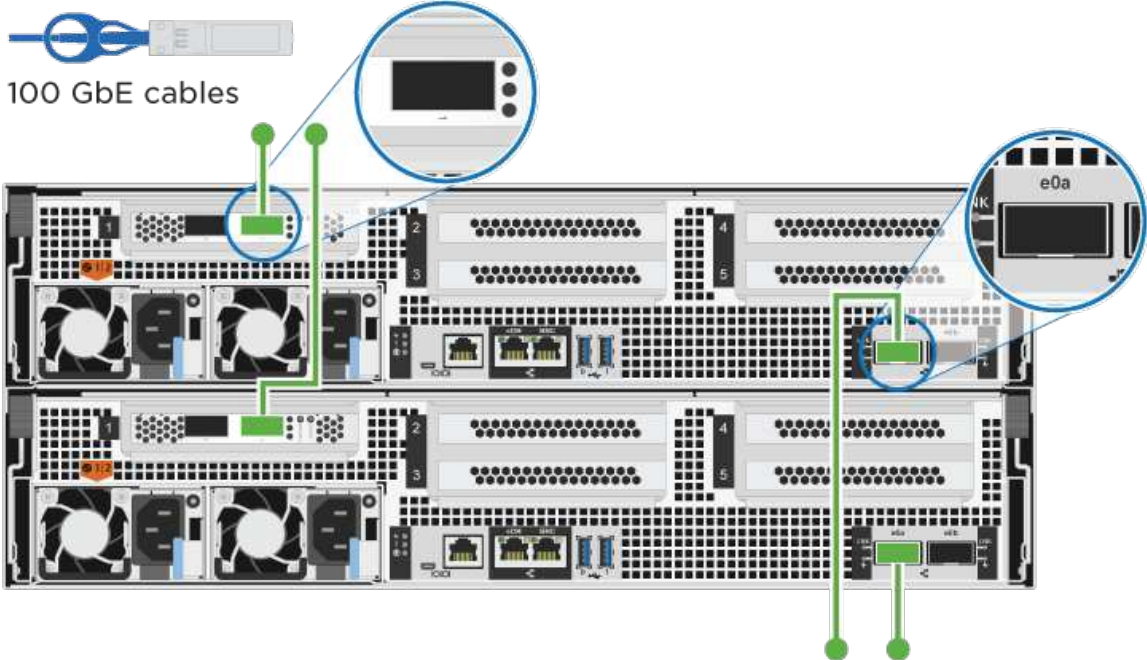



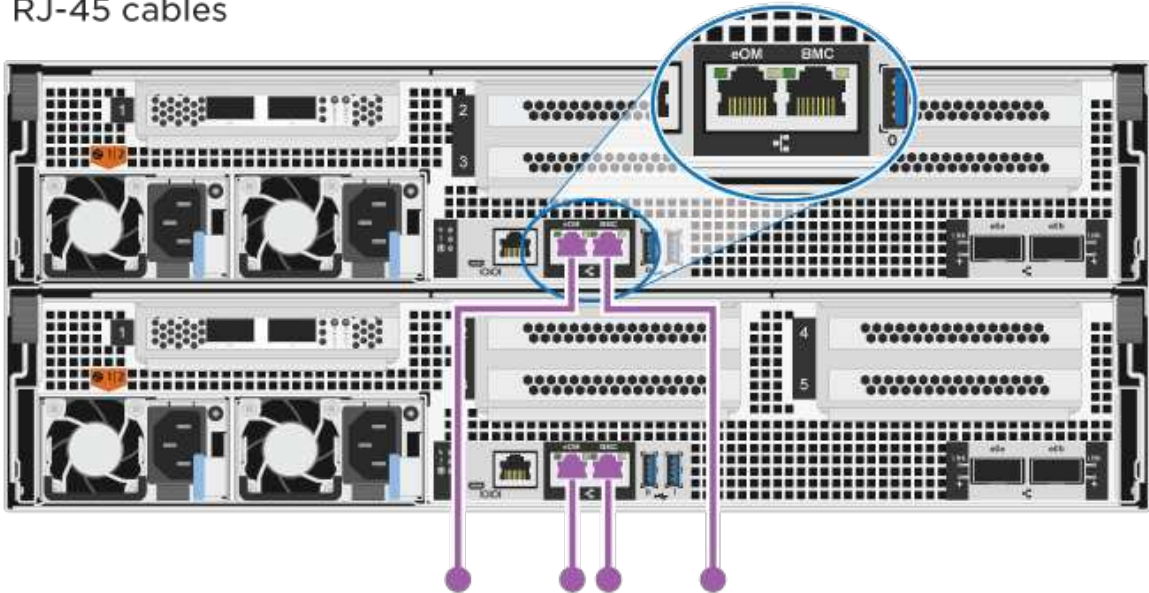

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Steps

1. Use the animation or the tabulated steps to complete the cabling between the controllers and the switches:

[Animation - Cable a switched cluster](#)

Step	Perform on each controller module
<div data-bbox="180 153 256 212">1</div>	<p data-bbox="313 153 716 195">Cable the HA interconnect ports:</p> <ul data-bbox="337 226 496 310" style="list-style-type: none"> • e0b to e0b • e1b to e1b <div data-bbox="331 363 1446 909">  <p data-bbox="331 457 553 489">100 GbE cables</p> </div>
<div data-bbox="180 978 256 1037">2</div>	<p data-bbox="313 978 1317 1020">Cable the cluster interconnect ports to the 100 GbE cluster interconnect switches.</p> <ul data-bbox="337 1052 412 1136" style="list-style-type: none"> • e0a • e1a <div data-bbox="331 1188 1471 1843">  <p data-bbox="331 1262 553 1293">100 GbE cables</p> </div>

Step	Perform on each controller module
3	<p>Cable the management ports to the management network switches</p> <p> RJ-45 cables</p> 
	DO NOT plug in the power cords at this point.

2. To perform optional cabling, see:

- [Option 1: Cable to a Fibre Channel host network](#)
- [Option 2: Cable to a 10GbE host network](#)
- [Option 3: Cable the controllers to a single drive shelf](#)
- [Option 4: Cable the controllers to two drive shelves](#)

3. 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.

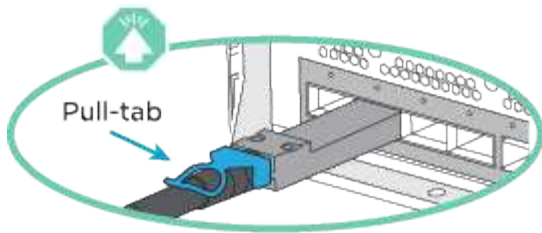
Option 1: Cable to a Fibre Channel host network

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	<p>Cable ports 2a through 2d to the FC host switches.</p>
2	<p>To perform other optional cabling, choose from:</p> <ul style="list-style-type: none"> • Option 3: Cable the controllers to a single drive shelf • Option 4: Cable the controllers to two drive shelves
3	<p>To complete setting up your system, see Step 4: Complete system setup and configuration.</p>

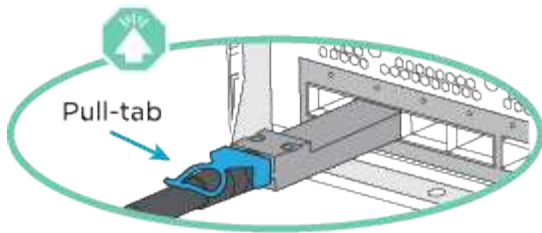
Option 2: Cable to a 10GbE host network

10GbE ports on the controllers are connected to 10GbE 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.

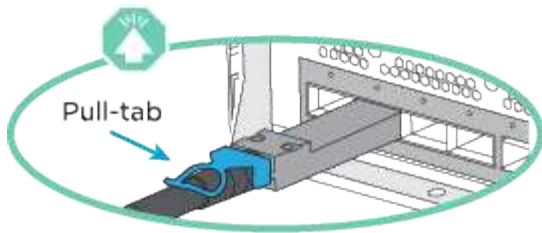
Step	Perform on each controller module
1	<p>Cable ports e4a through e4d to the 10GbE host network switches.</p> <p>10 GbE cables</p>
2	<p>To perform other optional cabling, choose from:</p> <ul style="list-style-type: none"> • Option 3: Cable the controllers to a single drive shelf • Option 4: Cable the controllers to two drive shelves
3	<p>To complete setting up your system, see Step 4: Complete system setup and configuration.</p>

Option 3: Cable the controllers to a single drive shelf

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

Before you begin

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

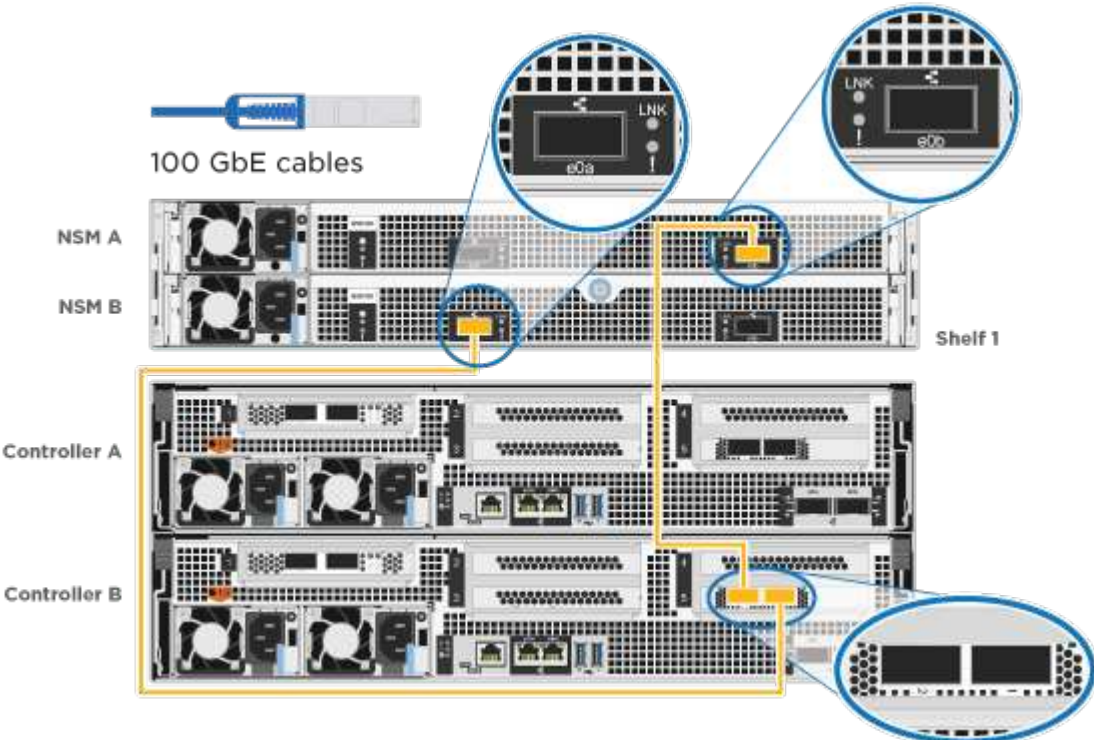


As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Use the animation or the tabulated steps to cable your controllers to a single shelf:

Animation - Cable the controllers to a single drive shelf

Step	Perform on each controller module
1	<p>Cable controller A to the shelf:</p> <p>The diagram illustrates the cabling process for a server rack. At the top, a blue 100 GbE cable is shown. Below it, the rack is divided into sections: NSM A, NSM B, Shelf 1, Controller A, and Controller B. Blue lines indicate the connection paths. From NSM A and NSM B, cables connect to Shelf 1. From Controller A and Controller B, cables connect to Shelf 1. Callouts show the physical connections: a cable plugged into a port on Shelf 1, a cable plugged into a port on Controller A, and a cable plugged into a port on Controller B.</p>

Step	Perform on each controller module
2	<p>Cable controller B to the shelf:</p>  <p>The diagram illustrates the cabling for Step 2. At the top, a blue cable is labeled '100 GbE cables'. Below it, 'Shelf 1' contains two NSM modules, NSM A and NSM B. Callouts show the LNK and SFP ports on these modules. Below Shelf 1 are two controller modules, Controller A and Controller B. A yellow line traces the path of the cables from the SFP ports on NSM B to the corresponding ports on Controller B. Another callout shows the ports on Controller B.</p>

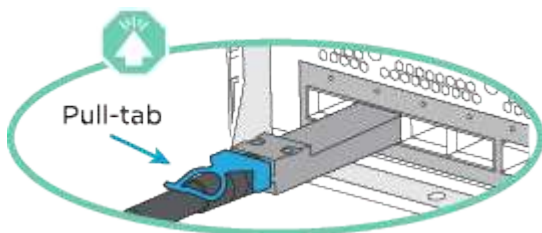
To complete setting up your system, see [Step 4: Complete system setup and configuration](#).

Option 4: Cable the controllers to two drive shelves

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

Before you begin

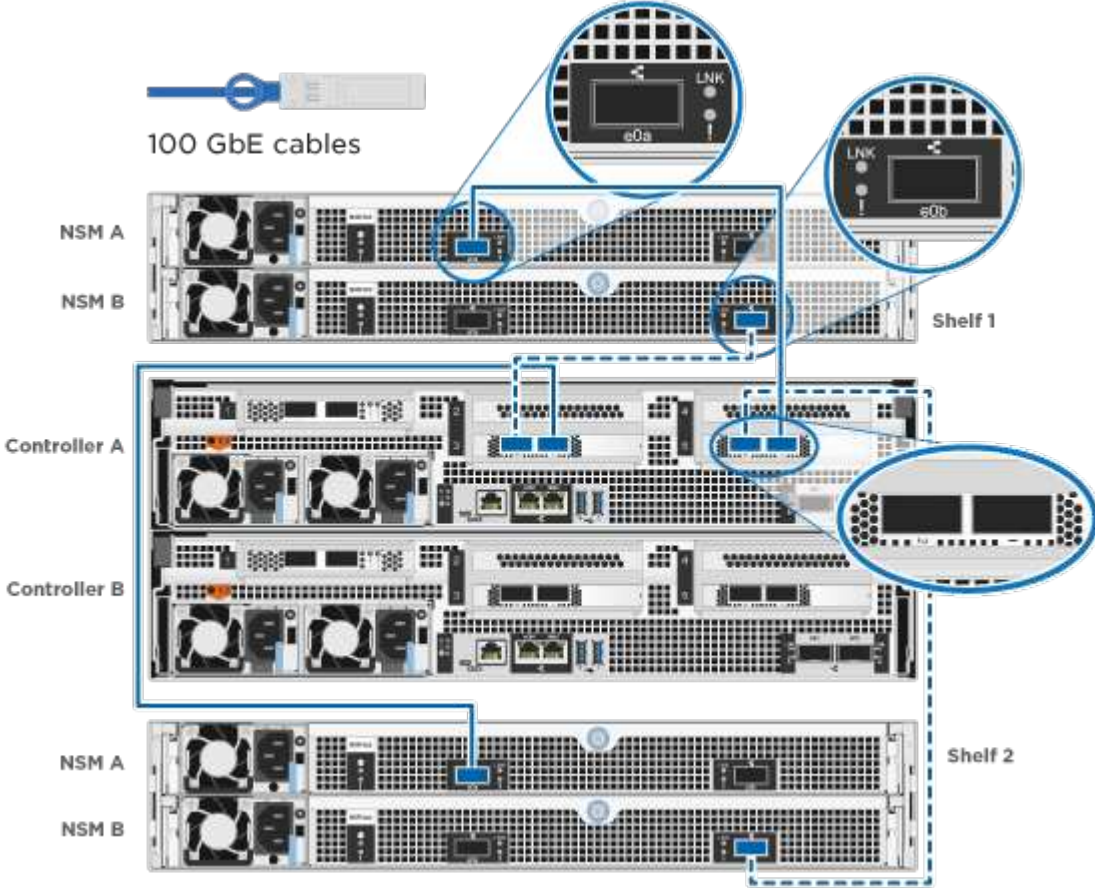
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.

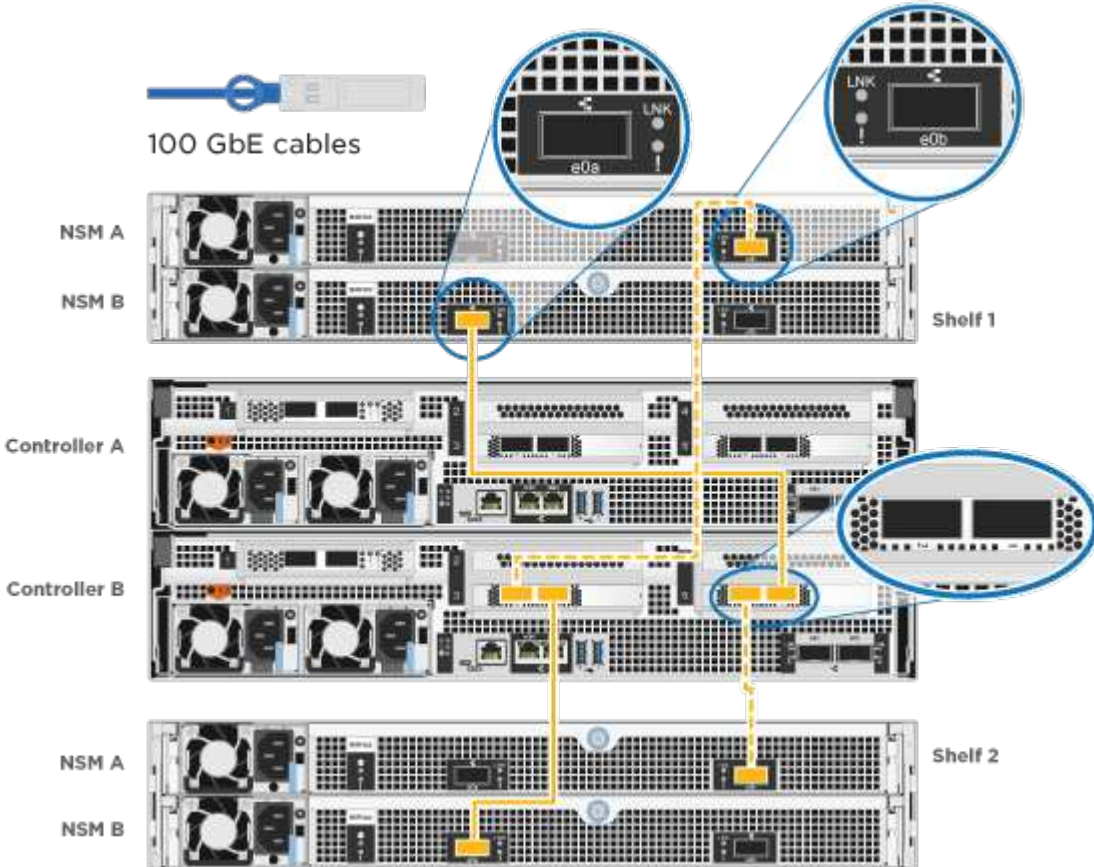


As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

Use the animation or the tabulated steps to cable your controllers to two drive shelves:

[Animation - Cable the controllers to two drive shelves](#)

Step	Perform on each controller module
<div data-bbox="131 163 207 210">1</div>	<p data-bbox="272 163 678 195">Cable controller A to the shelves:</p>  <p>The diagram illustrates the physical connection of 100 GbE cables between Controller A and the network shelf modules (NSM A and NSM B) across two shelves. Shelf 1 contains NSM A, NSM B, and Controller A. Shelf 2 contains NSM A and NSM B. Blue lines represent the cable connections. Callouts provide details of the ports: on the NSM modules, the 'LNK' (Link) and 'e0a' ports are shown; on Controller A, the corresponding ports are labeled '100GbE'.</p>

Step	Perform on each controller module
2	<p>Cable controller B to the shelves:</p>  <p>The diagram illustrates the physical connection of 100 GbE cables from Controller B to the network shelf modules (NSM A and NSM B) on Shelf 1 and Shelf 2. Shelf 1 also contains Controller A. Yellow lines trace the cable paths from the S0b ports on Controller B to the LNK ports on the NSM modules. Callouts provide a closer look at the port labels: 'LNK' and 'S0a' on the NSM modules, and 'LNK' and 'S0b' on Controller B.</p>

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.

The system begins to boot. Initial booting may take up to eight minutes.

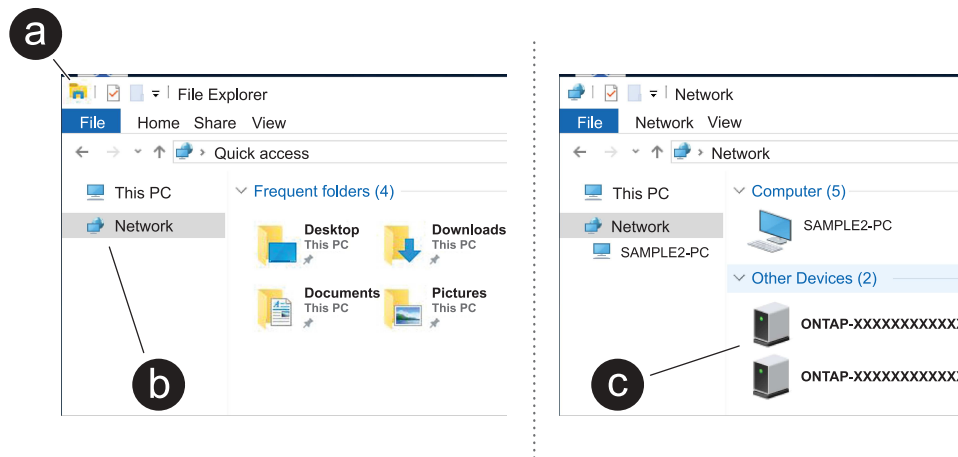
2. Make sure that your laptop has network discovery enabled.

See your laptop's online help for more information.

3. Use the animation to connect your laptop to the Management switch:

Animation - 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 and right-click and select **refresh**.
- c. 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 [ONTAP 9 documentation](#) 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.

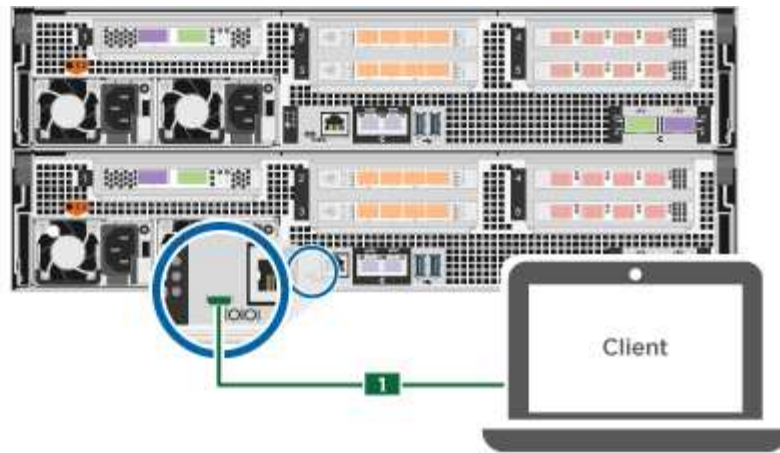
Steps

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.

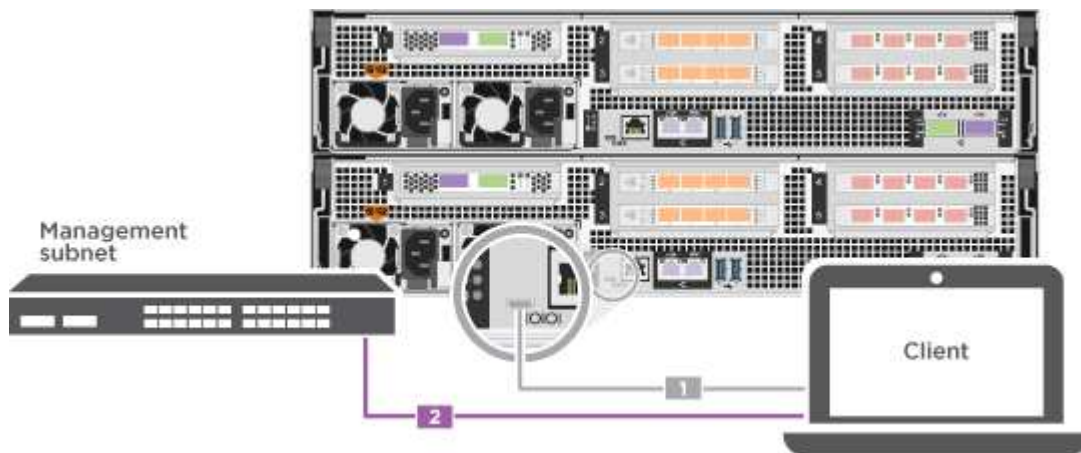


See your laptop or console's online help for how to configure the console port.

- b. Connect the 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. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.

The system begins to boot. Initial booting may take up to eight minutes.

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	<ol style="list-style-type: none"> a. Open a console session using PuTTY, a terminal server, or the equivalent for your environment. <div style="display: flex; align-items: center; margin: 10px 0;"> <div style="text-align: center; margin-right: 10px;">  </div> <div>Check your laptop or console's online help if you do not know how to configure PuTTY.</div> </div> <ol style="list-style-type: none"> 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 [ONTAP 9 documentation](#) for information about configuring additional features in ONTAP.

Maintain

Maintain ASA C800 hardware

Maintain the hardware of your ASA C800 storage system to ensure long-term reliability and optimal performance. Perform regular maintenance tasks such as replacing faulty components, as this helps prevent downtime and data loss.

The maintenance procedures assume that the ASA C800 storage system has already been deployed as a storage node in the ONTAP environment.

System components

For the ASA C800 storage system, you can perform maintenance procedures on the following components.

Boot media - automated recovery

The boot media stores a primary and secondary set of ONTAP image files that the storage system uses to boot. During automated recovery, the system retrieves the boot image from the partner node and automatically runs the appropriate boot menu option to install the image on your replacement boot media. The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the [manual boot recovery procedure](#).

Boot media - manual recovery

The boot media stores a primary and secondary set of ONTAP image files that the storage system uses to boot. During manual recovery, you boot the storage system from a USB drive and manually restore the file system image and configuration. If your storage system is running ONTAP 9.17.1 and later, use the [automated boot recovery procedure](#).

Chassis

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

Controller

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

DIMM

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

Drive

A drive is a device that provides the physical storage media for data.

Fan	The fan cools the controller.
NVDIMM	The NVDIMM (non-volatile dual in-line memory module) manages the data transfer from the volatile memory to the non-volatile storage, and maintains data integrity in the event of a power loss or system shutdown.
NVDIMM battery	A NVDIMM battery is responsible for maintaining power to the NVDIMM module.
PCIe card and risers	A PCIe (peripheral component interconnect express) card is an expansion card that plugs into the PCIe slot on the motherboard or into risers plugged into the motherboard.
Power supply	A power supply provides a redundant power source in a controller shelf.
Real-time clock battery	A real time clock battery preserves system date and time information if the power is off.

Boot media - automated recovery

Boot media automated recovery workflow - ASA C800

The automated recovery of the boot image involves the system automatically identifying and selecting the appropriate boot menu option. It uses the boot image on partner node to reinstall ONTAP on the replacement boot media in your ASA C800 storage system.

The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the [manual boot recovery procedure](#).

To get started, review the replacement requirements, shut down the controller, replace the boot media, allow the system to restore the image, and verify system functionality.

1

Review the boot media requirements

Review the requirements for boot media replacement.

2

Shut down the controller

Shut down the controller in your storage system when you need to replace the boot media.

3

Replace the boot media

Remove the failed boot media from the controller module and install the replacement boot media.

4

Restore the image on the boot media

Restore the ONTAP image from the partner controller.

Return the failed part to NetApp

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

Requirements for automated boot media recovery - ASA C800

Before replacing the boot media in your ASA C800, ensure you meet the necessary requirements for a successful replacement. This includes verifying that you have the correct replacement boot media, confirming that the e0S (e0M wrench) port on the impaired controller is not faulty, and determining whether Onboard Key Manager (OKM) or External Key Manager (EKM) is enabled.

The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the [manual boot recovery procedure](#).

- You must replace the failed component with a replacement FRU component of the same capacity that you received from NetApp.
- Verify that the e0M (wrench) port on the impaired controller is connected and not faulty.

The e0M port is used to communicate between the two controllers during the automated boot recovery process.

- For OKM, you need the cluster-wide passphrase and also the backup data.
- For EKM, you need copies of the following files from the partner node:
 - /cfcard/kmip/servers.cfg file.
 - /cfcard/kmip/certs/client.crt file.
 - /cfcard/kmip/certs/client.key file.
 - /cfcard/kmip/certs/CA.pem file.
- It is critical to apply the commands to the correct controller when you are replacing the impaired boot media:
 - The *impaired controller* is the controller on which you are performing maintenance.
 - The *healthy controller* is the HA partner of the impaired controller.

What's next

After you've reviewed the boot media requirements, you [shut down the controller](#).

Shut down the controller for automated boot media recovery - ASA C800

Shut down the impaired controller in your ASA C800 storage system to prevent data loss and maintain system stability during the automated boot media recovery process.

The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the [manual boot recovery procedure](#).

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <code>-halt true</code> parameter brings you to the LOADER prompt.</p>

What's next

After you shut down the impaired controller, you [replace the boot media](#).

Replace the boot media for automated boot recovery - ASA C800

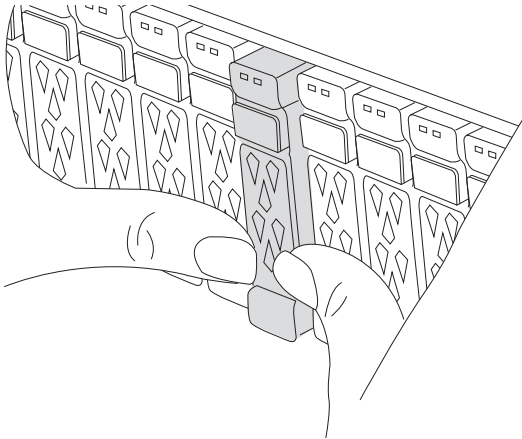
The boot media in your ASA C800 system stores essential firmware and configuration data. The replacement process involves removing and opening the controller module,

removing the impaired boot media, installing the replacement boot media in the controller module, and then reinstalling the controller module.

The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the [manual boot recovery procedure](#).

The boot media is located inside the controller module under the air duct, and is accessed by removing the controller module from the system.

1. If you are not already grounded, properly ground yourself.
2. Ensure that all drives in the chassis are firmly seated against the midplane by using your thumbs to push each drive until you feel a positive stop.

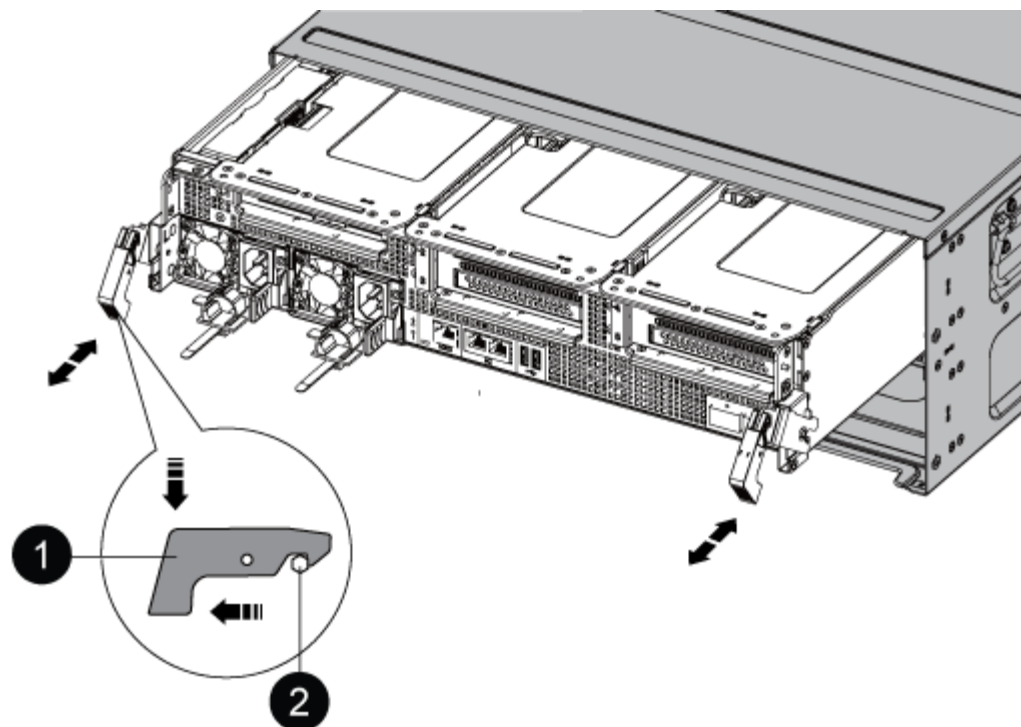


3. Unplug the controller module power supplies from the source.
4. Release the power cable retainers, and then unplug the cables from the power supplies.
5. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if 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.

6. Remove the cable management device from the controller module and set it aside.
7. 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.



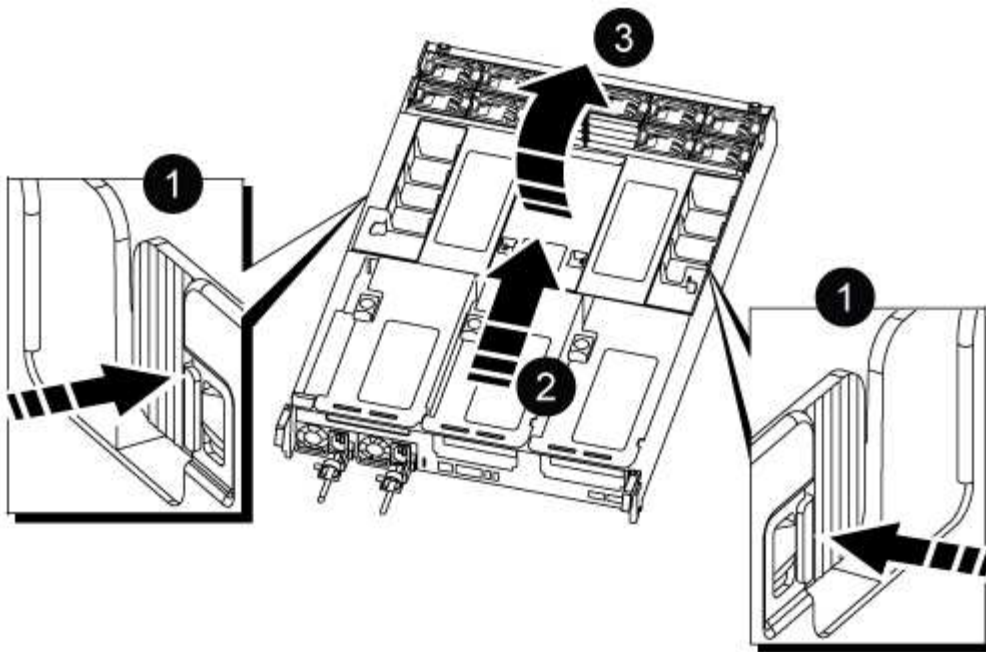
1	Locking latch
2	Locking pin

8. 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.

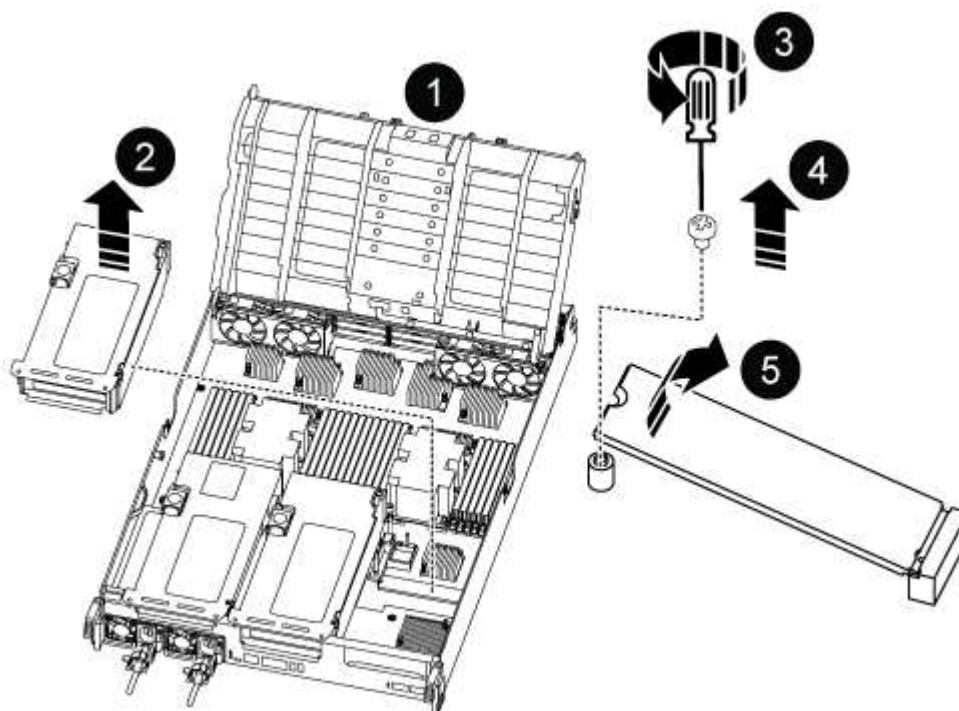
9. Place the controller module on a stable, flat surface, and then open the air duct:

- Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
- Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.



1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

10. Locate the boot media in the controller module and replace it:



1	Air duct
2	Riser 3
3	Phillips #1 screwdriver
4	Boot media screw
5	Boot media

- a. Using a #1 Phillips head screwdriver, remove the screw holding down the boot media and set the screw aside in a safe place.
- b. Grasping the sides of the boot media, gently rotate the boot media up, and then pull the boot media straight out of the socket and set it aside.

11. Install the replacement boot media into the controller module:

- a. Align the edges of the boot media with the socket housing, and then gently push it squarely into the socket.
- b. Rotate the boot media down toward the motherboard.
- c. Secure the boot media to the motherboard using the boot media screw.

Do not over-tighten the screw or you might damage the boot media.

12. Reinstall the riser into the controller module.

13. Close the air duct:

- a. Rotate the air duct downward.
- b. Slide the air duct toward the risers until it clicks into place.

14. Install the controller module:

- a. Align the end of the controller module with the opening in the chassis, and then gently push the controller module half-way into the way into the system.
- b. Recable the controller module, 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 module begins to boot and stops at the LOADER prompt.

What's next

After physically replacing the impaired boot media, [restore the ONTAP image from the partner node](#).

Automated boot media recovery from the partner node - ASA C800

After installing the new boot media device in your ASA C800 system, you can start the automated boot media recovery process to restore the configuration from the partner node. During the recovery process, the system checks whether encryption is enabled and

determines the type of key encryption in use. If key encryption is enabled, the system guides you through the appropriate steps to restore it.

The automated boot media recovery process is supported only in ONTAP 9.17.1 and later. If your storage system is running an earlier version of ONTAP, use the [manual boot recovery procedure](#).

Before you begin

- For OKM, you need the cluster-wide passphrase and also the backup data.
- For EKM, you need copies of the following files from the partner node:
 - /cfcard/kmip/servers.cfg file.
 - /cfcard/kmip/certs/client.crt file.
 - /cfcard/kmip/certs/client.key file.
 - /cfcard/kmip/certs/CA.pem file.

Steps

1. From the LOADER prompt, enter the command:

```
boot_recovery -partner
```

The screen displays the following message:

```
Starting boot media recovery (BMR) process. Press Ctrl-C to abort...
```

2. Monitor the boot media install recovery process.

The process completes and displays the `Installation complete` message.

3. The system checks for encryption and encryption type and displays one of two messages. Depending on what message is displayed, take one of the following actions:



Occasionally, the process may not be able to identify if key manager is configured on the system. It will display an error message, ask if key manager is configured for the system, and then ask what type of key manager is configured. The process will resume after you resolve the issue.

Show example of configuration error finding prompts

```
Error when fetching key manager config from partner ${partner_ip}:  
${status}
```

```
Has key manager been configured on this system
```

```
Is the key manager onboard
```

If you see this message...	Do this...
key manager is not configured. Exiting.	<p>Encryption is not installed on the system. Complete the following steps:</p> <ol style="list-style-type: none"> Log into the node when the login prompt is displayed and give back the storage: <pre>storage failover giveback -ofnode impaired_node_name</pre> Go to step 5 to enable automatic giveback if it was disabled.
key manager is configured.	<p>Go to step 4 to restore the appropriate key manager.</p> <p>The node accesses the boot menu and runs:</p> <ul style="list-style-type: none"> Option 10 for systems with Onboard Key Manager (OKM). Option 11 for systems with External Key Manager (EKM).

4. Select the appropriate key manager restoration process.

Onboard Key Manager (OKM)

If OKM is detected, the system displays the following message and begins running BootMenu Option 10.

```
key manager is configured.  
Entering Bootmenu Option 10...
```

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

- a. Enter `y` at the prompt to confirm you want to start the OKM recovery process.
- b. Enter the following when prompted:
 - i. The passphrase
 - ii. The passphrase again when prompted to confirm
 - iii. Backup data for onboard key manager

Show example of passphrase and backup data prompts

```
Enter the passphrase for onboard key management:  
-----BEGIN PASSPHRASE-----  
<passphrase_value>  
-----END PASSPHRASE-----  
Enter the passphrase again to confirm:  
-----BEGIN PASSPHRASE-----  
<passphrase_value>  
-----END PASSPHRASE-----  
Enter the backup data:  
-----BEGIN BACKUP-----  
<passphrase_value>  
-----END BACKUP-----
```

- c. Continue to monitor the recovery process as it restores the appropriate files from the partner node.

When the recovery process is complete, the node will reboot. The following messages indicate a successful recovery:

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

Successfully recovered keymanager secrets.
```

d. When the node reboots, verify the boot media recovery was successful by confirming that the system is back online and operational.

e. Return the impaired controller to normal operation by giving back its storage:

```
storage failover giveback -ofnode impaired_node_name
```

f. After the partner node is fully up and serving data, synchronize the OKM keys across the cluster.

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

External Key Manager (EKM)

If EKM is detected, the system displays the following message and begins running BootMenu Option 11.

```
key manager is configured.
Entering Bootmenu Option 11...
```

a. The next step depends on which version of ONTAP your system is running:

If your system is running...	Do this...
ONTAP 9.16.0	<p>a. Press <code>Ctlr-C</code> to exit BootMenu Option 11.</p> <p>b. Press <code>Ctlr-C</code> to exit the EKM configuration process and return to the boot menu.</p> <p>c. Select BootMenu Option 8.</p> <p>d. Reboot the node.</p> <p>If AUTOBOOT is set, the node reboots and uses the configuration files from the partner node.</p> <p>If AUTOBOOT is not set, enter the appropriate boot command. The node reboots and uses the configuration files from the partner node.</p> <p>e. Reboot the node so that EKM protects the boot media partition.</p> <p>f. Proceed to step c.</p>

If your system is running...	Do this...
ONTAP 9.16.1 and later	Proceed to the next step.

b. Enter the following EKM configuration setting when prompted:

Action	Example
Enter the client certificate contents from the /cfcard/kmip/certs/client.crt file.	Show example of client certificate contents <pre> -----BEGIN CERTIFICATE----- <certificate_value> -----END CERTIFICATE----- </pre>
Enter the client key file contents from the /cfcard/kmip/certs/client.key file.	Show example of client key file contents <pre> -----BEGIN RSA PRIVATE KEY----- <key_value> -----END RSA PRIVATE KEY----- </pre>
Enter the KMIP server CA(s) file contents from the /cfcard/kmip/certs/CA.pem file.	Show example of KMIP server file contents <pre> -----BEGIN CERTIFICATE----- <KMIP_certificate_CA_value > -----END CERTIFICATE----- </pre>

Action	Example
<p>Enter the server configuration file contents from the /cfcard/kmip/servers.cfg file.</p>	<p>Show example of server configuration file contents</p> <pre> xxx.xxx.xxx.xxx:5696.host= xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx:5696.port= 5696 xxx.xxx.xxx.xxx:5696.trusted_file=/cfcard/kmip/certs/CA.pem xxx.xxx.xxx.xxx:5696.protocol=KMIP1_4 1xxx.xxx.xxx.xxx:5696.timeout=25 xxx.xxx.xxx.xxx:5696.nbio=1 xxx.xxx.xxx.xxx:5696.cert_file=/cfcard/kmip/certs/client.crt xxx.xxx.xxx.xxx:5696.key_file=/cfcard/kmip/certs/client.key xxx.xxx.xxx.xxx:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:!RC2:!RC4:!SEED:!eNULL:!aNULL" xxx.xxx.xxx.xxx:5696.verify=true xxx.xxx.xxx.xxx:5696.netapp_keystore_uuid=<id_value> </pre>

Action	Example
<p>If prompted, enter the ONTAP Cluster UUID from the partner.</p> <p>You can check the cluster UUID from the partner node using the <code>cluster identify show</code> command.</p>	<p>Show example of ONTAP Cluster UUID</p> <div data-bbox="898 233 1425 730" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Notice:</p> <pre>bootarg.mgwd.cluster_uuid is not set or is empty. Do you know the ONTAP Cluster UUID? {y/n} y Enter the ONTAP Cluster UUID: <cluster_uuid_value></pre> <p>System is ready to utilize external key manager(s).</p> </div>
<p>If prompted, enter the temporary network interface and settings for the node.</p> <p>You need to enter:</p> <ol style="list-style-type: none"> 1. The IP address for the port 2. The netmask for the port 3. The IP address of the default gateway 	<p>Show example of a temporary network setting</p> <div data-bbox="898 884 1425 1864" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>In order to recover key information, a temporary network interface needs to be configured.</p> <p>Select the network port you want to use (for example, 'e0a')</p> <pre>e0M</pre> <p>Enter the IP address for port : xxx.xxx.xxx.xxx</p> <p>Enter the netmask for port : xxx.xxx.xxx.xxx</p> <p>Enter IP address of default gateway: xxx.xxx.xxx.xxx</p> <p>Trying to recover keys from key servers....</p> <pre>[discover_versions] [status=SUCCESS reason=message=]</pre> </div>

c. Depending on whether the key is successfully restored, take one of the following actions:

- If you see `kmip2_client: Successfully imported the keys from external key server: xxx.xxx.xxx.xxx:5696` in the output, the EKM configuration has been successfully restored.

The process attempts to restore the appropriate files from the partner node and reboots the node. Go to step d.

- If the key is not successfully restored, the system will halt and indicate that it could not restore the key. The error and warning messages are displayed. You must rerun the recovery process:

```
boot_recovery -partner
```

Show example of key recovery error and warning messages

```
ERROR: kmip_init: halting this system with encrypted
mroot...
WARNING: kmip_init: authentication keys might not be
available.
*****
*                               A T T E N T I O N                               *
*                                                                                   *
*          System cannot connect to key managers.          *
*                                                                                   *
*****
ERROR: kmip_init: halting this system with encrypted
mroot...
.
Terminated

Uptime: 11m32s
System halting...

LOADER-B>
```

d. When the node reboots, verify that the boot media recovery was successful by confirming that the system is back online and operational.

e. 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
```

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

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

What's next

After you've restored the ONTAP image and the node is up and serving data, you [return the failed part to NetApp](#).

Return the failed boot media to NetApp - ASA C800

If a component in your ASAF C800 system fails, return the failed part to NetApp. See the [Part Return and Replacements](#) page for further information.

Boot media - manual recovery

Boot media manual recovery workflow - ASA C800

Get started with replacing the boot media in your ASA C800 storage system by reviewing the replacement requirements, checking encryption status, shutting down the controller, replacing the boot media, booting the recovery image, restoring encryption, and verifying the system functionality.

If your storage system is running ONTAP 9.17.1 or later, use the [manual boot recovery procedure](#)

1

Review the boot media requirements

Review the requirements for replacing the boot media.

2

Check encryption key support and status

Determine whether the system has security key manager enabled or encrypted disks.

3

Shut down the controller

Shut down the controller when when you need to replace the boot media.

4

Replace the boot media

Remove the failed boot media from the System Management module and install the replacement boot media, and then transfer an ONTAP image using a USB flash drive.

5

Boot the recovery image

Boot the ONTAP image from the USB drive, restore the file system, and verify the environmental variables.

6

Restore encryption

Restore the onboard key manager configuration or the external key manager from the ONATP boot menu.

7

Return the failed part to NetApp

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

Requirements for manual boot media recovery - ASA C800

Before replacing the boot media in your ASA C800 system, ensure you meet the necessary requirements for a successful replacement. This includes making sure you have a USB flash drive with the appropriate amount of storage and verifying that you have the correct replacement boot device.

If your storage system is running ONTAP 9.17.1 or later, use the [manual boot recovery procedure](#)

USB flash drive

- Ensure you have a USB flash drive formatted to FAT32.
- The USB must have sufficient storage capacity to hold the `image_xxx.tgz` file.

File preparation

Copy the `image_xxx.tgz` file to the USB flash drive. This file will be used when you transfer the ONTAP image using the USB flash drive.

Component replacement

Replace the failed component with the replacement component provided by NetApp.

Controller identification

It is critical to apply the commands to the correct controller when you are replacing the impaired boot media:

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

What's next?

After you've reviewed the requirements to replace the boot media, you need to [check encryption key support and status on the boot media](#).

Check encryption key support and status - ASA C800

To ensure data security on your storage system, you need to verify the encryption key support and status on your boot media. Check if your ONTAP version supports NetApp Volume Encryption (NVE), and before you shut down the controller check if the key manager is active.

If your storage system is running ONTAP 9.17.1 or later, use the [manual boot recovery procedure](#)

Step 1: Check if your version of ONTAP supports NetApp Volume Encryption

Check whether your ONTAP version supports NetApp Volume Encryption (NVE). This information is crucial for downloading the correct ONTAP image.

Steps

1. Determine if your ONTAP version supports encryption by running the following command:

```
version -v
```

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

2. Depending on whether NVE is supported on your system, take one of the following actions:
 - If NVE is supported, download the ONTAP image with NetApp Volume Encryption.
 - If NVE is not supported, download the ONTAP image **without** NetApp Volume Encryption.

Step 2: Determine if it is safe to shut down the controller

To safely shut down a controller, first identify whether the External Key Manager (EKM) or the Onboard Key Manager (OKM) is active. Then, verify the key manager in use, display the appropriate key information, and take action based on the status of the authentication keys.

Steps

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

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

2. Depending on whether a key manger is configured on your system, select one of the following options.

No key manager configured

You can safely shut down the impaired controller. Go to [shutdown the impaired controller](#).

External or Onboard key manager configured

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

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

- b. Check the output for the value in the `Restored` column for your key manager.

This column indicates whether the authentication keys for your key manager (either EKM or OKM) have been successfully restored.

3. Depending on whether your system is using the External Key Manager or Onboard Key Manager, select one of the following options.

External Key Manager

Depending on the output value displayed in the `Restored` column, follow the appropriate steps.

Output value in <code>Restored</code> column	Follow these steps...
<code>true</code>	You can safely shut down the impaired controller. Go to shutdown the impaired controller .
Anything other than <code>true</code>	<ol style="list-style-type: none">Restore the external key management authentication keys to all nodes in the cluster using the following command: <pre>security key-manager external restore</pre> If the command fails, contact NetApp Support.Verify that the <code>Restored</code> column displays <code>true</code> for all authentication keys by entering the <code>security key-manager key query</code> command. If all the authentication keys are <code>true</code>, you can safely shut down the impaired controller. Go to shutdown the impaired controller.

Onboard Key Manager

Depending on the output value displayed in the `Restored` column, follow the appropriate steps.

Output value in <code>Restored</code> column	Follow these steps...
<code>true</code>	<p>Manually back up the OKM information.</p> <ol style="list-style-type: none">Go to the advanced mode by entering <code>set -priv advanced</code> and then enter <code>Y</code> when prompted.Enter the following command to display the key management information: <pre>security key-manager onboard show-backup</pre>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.You can safely shut down the impaired controller. Go to shutdown the impaired controller.

Output value in Restored column	Follow these steps...
Anything other than true	<p>a. Enter the onboard security key-manager sync command:</p> <pre>security key-manager onboard sync</pre> <p>b. Enter the 32 character, alphanumeric onboard key management passphrase when prompted.</p> <p>If the passphrase cannot be provided, contact NetApp Support.</p> <p>c. Verify the Restored column displays true for all authentication keys:</p> <pre>security key-manager key query</pre> <p>d. Verify that the Key Manager type displays onboard, and then manually back up the OKM information.</p> <p>e. Enter the command to display the key management backup information:</p> <pre>security key-manager onboard show-backup</pre> <p>f. Copy the contents of the backup information to a separate file or your log file.</p> <p>You'll need it in disaster scenarios where you might need to manually recover OKM.</p> <p>g. You can safely shut down the impaired controller. Go to shutdown the impaired controller.</p>

Shut down the controller for manual boot media recovery - ASA C800

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.

If your storage system is running ONTAP 9.17.1 or later, use the [automated boot recovery procedure](#). If your system is running an earlier version of ONTAP, you must use the manual boot recovery procedure.

Option 1: Most systems

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

Steps

- Take the impaired controller to the LOADER prompt:

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

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



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

Option 2: System 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 [Synchronize a node with the cluster](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

Steps

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

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

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Disable automatic giveback from the console of the healthy controller: `storage failover modify -node local -auto-giveback false`
3. Take the impaired controller to the LOADER prompt:

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

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

Replace the boot media and prepare for manual boot recovery - ASA C800

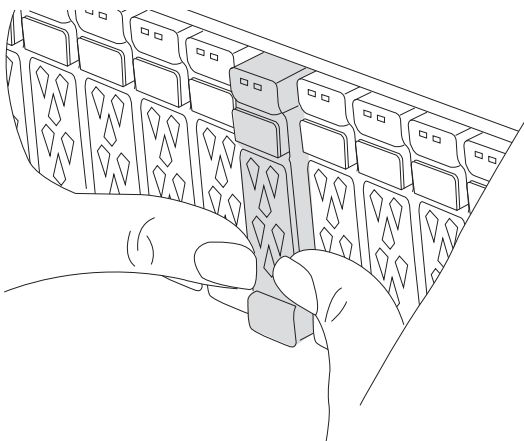
To replace the boot media, you must remove the impaired controller module, install the replacement boot media, and transfer the boot image to a USB flash drive.

If your storage system is running ONTAP 9.17.1 or later, use the automated boot recovery procedure. If your system is running an earlier version of ONTAP, you must use the manual boot recovery process.

Step 1: Remove the controller module

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

1. If you are not already grounded, properly ground yourself.
2. Ensure that all drives in the chassis are firmly seated against the midplane by using your thumbs to push each drive until you feel a positive stop.



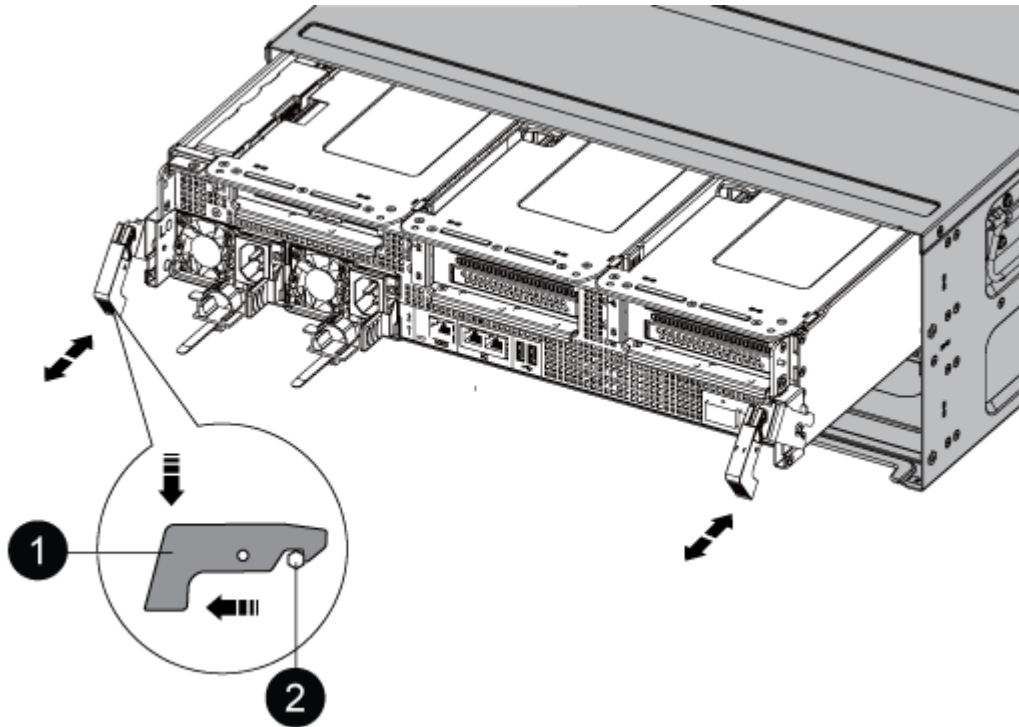
3. Unplug the controller module power supplies from the source.
4. Release the power cable retainers, and then unplug the cables from the power supplies.
5. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if 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.

6. Remove the cable management device from the controller module and set it aside.
7. 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.

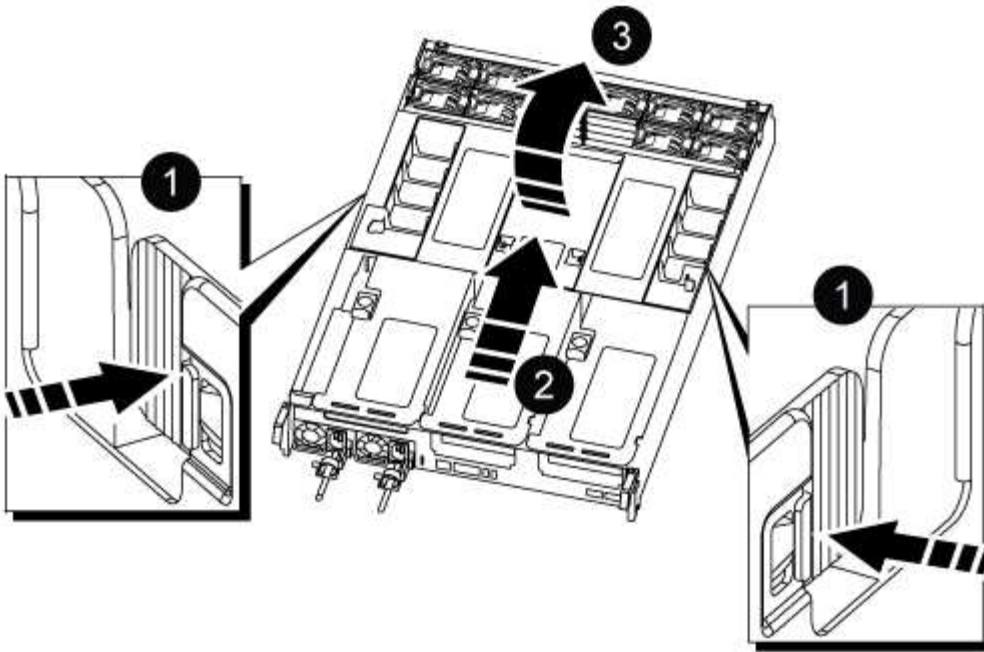


1	Locking latch
2	Locking pin

8. 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.

9. Place the controller module on a stable, flat surface, and then open the air duct:
 - a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
 - b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.



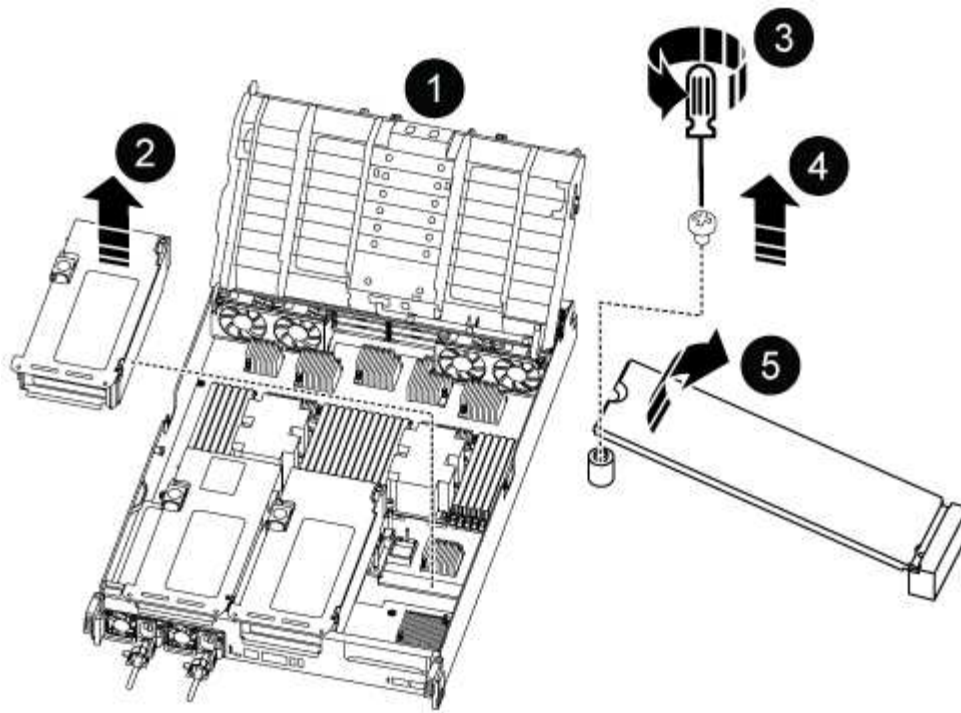
1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

Step 2: Replace the boot media

You locate the failed boot media in the controller module by removing Riser 3 on the controller module before you can replace the boot media.

You need a Phillips head screwdriver to remove the screw that holds the boot media in place.

1. Locate the boot media:



1	Air duct
2	Riser 3
3	Phillips #1 screwdriver
4	Boot media screw
5	Boot media

2. Remove the boot media from the controller module:

- Using a #1 Phillips head screwdriver, remove the screw holding down the boot media and set the screw aside in a safe place.
- Grasping the sides of the boot media, gently rotate the boot media up, and then pull the boot media straight out of the socket and set it aside.

3. Install the replacement boot media into the controller module:

- Align the edges of the boot media with the socket housing, and then gently push it squarely into the socket.
- Rotate the boot media down toward the motherboard.
- Secure the boot media to the motherboard using the boot media screw.

Do not over-tighten the screw or you might damage the boot media.

4. Reinstall the riser into the controller module.

5. Close the air duct:
 - a. Rotate the air duct downward.
 - b. Slide the air duct toward the risers until it clicks into place.

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.

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 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.
 - 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.

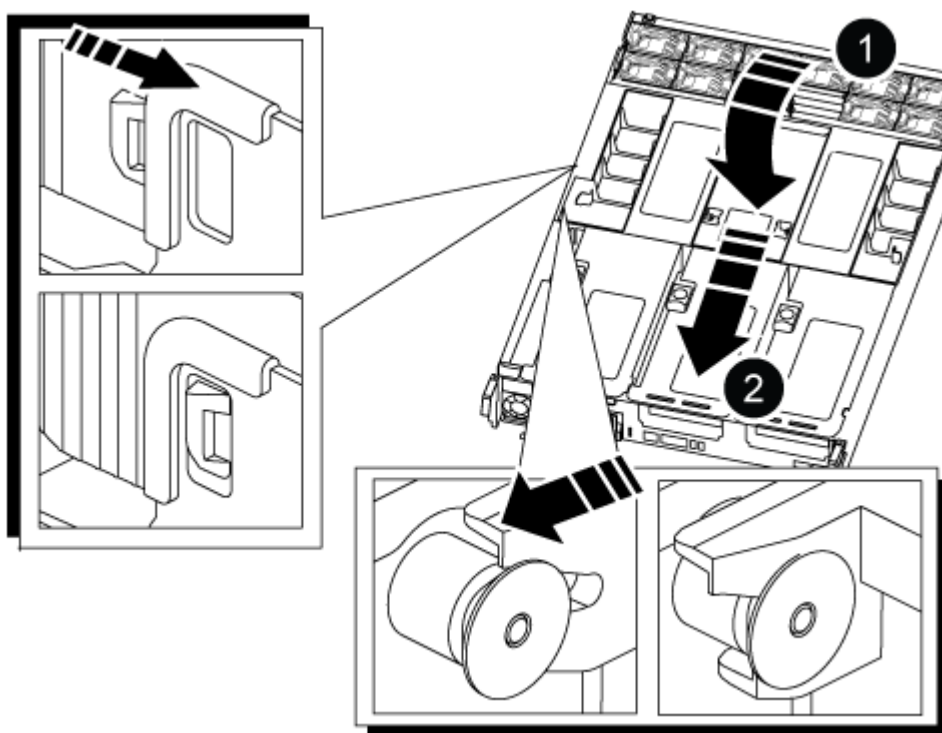


If the service image has no efi folder, see [EFI folder missing from Service Image download file used for boot device recovery for FAS and AFF models^](#).

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

- a. Remove the USB flash drive from your laptop.
2. If you have not already done so, close the air duct:
 - a. Swing the air duct all the way down to the controller module.
 - b. Slide the air duct toward the risers until the locking tabs click into place.

- c. Inspect the air duct to make sure that it is properly seated and locked into place.



1	Air duct
2	Risers

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. 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.

6. Gently push the controller module all the way into the system until the controller module locking hooks begin to rise, firmly push on the locking hooks to finish seating the controller module, and then swing the locking hooks into the locked position over the pins on the controller module.
7. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

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.

Manual boot media recovery from a USB drive - ASA C800

After installing the new boot media device in your system, you can boot the recovery image from a USB drive and restore the configuration from the partner node.

If your storage system is running ONTAP 9.17.1 or later, use the [manual boot recovery procedure](#)

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:

Option 1: ONTAP 9.16.0 or earlier

- a. On the impaired controller, press `Y` when you see `Do you want to restore the backup configuration now?`
- b. If prompted on the impaired controller, press `Y` to overwrite `/etc/ssh/ssh_host_ecdsa_key`.
- c. On the healthy partner controller, set the impaired controller to advanced privilege level: `set -privilege advanced`.
- d. On the healthy partner controller, run the restore backup command: `system node restore-backup -node local -target-address impaired_node_IP_address`.

NOTE: If you see any message other than a successful restore, contact [NetApp Support](#).

- e. On the healthy partner controller, return the impaired controller to admin level: `set -privilege admin`.
- f. On the impaired controller, press `Y` when you see `Was the restore backup procedure successful?`.
- g. On the impaired controller, press `Y` when you see `...would you like to use this restored copy now?`.
- h. On the impaired controller, press `Y` when prompted to reboot the impaired controller and press `ctrl-c` for the Boot Menu.
- i. If the system does not use encryption, select *Option 1 Normal Boot.*, otherwise go to [Restore encryption](#).

Option 2: ONTAP 9.16.1 or later

- a. On the impaired controller, press `Y` when prompted to restore the backup configuration.

After restore procedure is successful, this message will be seen on the console -
`syncflash_partner: Restore from partner complete.`

- b. On the impaired controller, press `Y` when prompted to confirm if the restore backup was successful.
- c. On the impaired controller, press `Y` when prompted to use the restored configuration.
- d. On the impaired controller, press `Y` when prompted to reboot the node.
- e. On the impaired controller, press `Y` when prompted to reboot the impaired controller and press `ctrl-c` for the Boot Menu.
- f. If the system does not use encryption, select *Option 1 Normal Boot.*, otherwise go to [Restore encryption](#).

4. Connect the console cable to the partner controller.
5. Give back the controller using the `storage failover giveback -fromnode local` command.
6. Restore automatic giveback if you disabled it by using the `storage failover modify -node local -auto-giveback true` command.
7. If AutoSupport is enabled, restore/unsuppress automatic case creation by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.

NOTE: If the process fails, contact [NetApp Support](#).

Restore encryption - ASA C800

Restore encryption on the replacement boot media.

If your storage system is running ONTAP 9.17.1 or later, use the [manual boot recovery procedure](#)

You must complete steps specific to systems that have Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) enabled using the settings that you captured at the beginning of the boot media replace procedure.

Depending on which a key manger is configured on your system, select one of the following options to restore it from the boot menu.

- [Option 1: Restore the Onboard Key Manager configuration](#)
- [Option 2: Restore the External Key Manager configuration](#)

Option 1: Restore the Onboard Key Manager configuration

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

Before you begin

- Make sure you have following information while restoring the OKM configuration:
 - Cluster-wide passphrase entered [while enabling onboard key management](#).
 - [Backup information for the Onboard Key Manager](#).
- Perform the [How to verify onboard key management backup and cluster-wide passphrase](#) procedure before proceeding.

Steps

1. Connect the console cable to the target controller.
2. From the ONTAP boot menu select the appropriate option from the boot menu.

ONTAP version	Select this option
ONTAP 9.8 or later	<p data-bbox="621 153 829 191">Select option 10.</p> <p data-bbox="621 222 948 254">Show example boot menu</p> <div data-bbox="654 296 1456 1081"> <p data-bbox="683 331 1294 363">Please choose one of the following:</p> <ul data-bbox="683 411 1369 1003" style="list-style-type: none"> <li data-bbox="683 411 971 443">(1) Normal Boot. <li data-bbox="683 453 1133 485">(2) Boot without /etc/rc. <li data-bbox="683 495 1045 527">(3) Change password. <li data-bbox="683 537 1369 600">(4) Clean configuration and initialize all disks. <li data-bbox="683 611 1149 642">(5) Maintenance mode boot. <li data-bbox="683 653 1328 684">(6) Update flash from backup config. <li data-bbox="683 695 1240 726">(7) Install new software first. <li data-bbox="683 737 971 768">(8) Reboot node. <li data-bbox="683 779 1192 842">(9) Configure Advanced Drive Partitioning. <li data-bbox="683 852 1333 915">(10) Set Onboard Key Manager recovery secrets. <li data-bbox="683 926 1317 989">(11) Configure node for external key management. <p data-bbox="683 1014 1032 1045">Selection (1-11)? 10</p> </div>

ONTAP version	Select this option
ONTAP 9.7 and earlier	<p>Select the hidden option <code>recover_onboard_keymanager</code></p> <p>Show example boot menu</p> <div> <pre> Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager </pre> </div>

3. Confirm that you want to continue the recovery process.

Show example prompt

```

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

```

4. Enter the cluster-wide passphrase twice.

While entering the passphrase the console will not show any input.

Show example prompt

```

Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:

```

5. Enter the backup information.

a. Paste the entire content from the BEGIN BACKUP line through the END BACKUP line.

Show example prompt

Enter the backup data:

```
-----BEGIN BACKUP-----
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----
```

b. Press the enter key twice at the end of the input.

The recovery process completes.

Show example prompt

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

Successfully recovered keymanager secrets.

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



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

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

Show example prompt

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

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

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

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

8. From the partner node, giveback the partner controller by entering the following command.

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

9. After booting with only the CFO aggregate, run the following command.

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

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

Show example prompt

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

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



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

11. Ensure that all keys are synced by entering the following command.

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

There are no entries matching your query.



No results should appear when filtering for false in the restored parameter.

12. Giveback the node from the partner by entering the following command.

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

13. Restore automatic giveback, if you disabled it, by entering the following command.

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

14. If AutoSupport is enabled, restore automatic case creation by entering the following command.

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

Option 2: Restore the External Key Manager configuration

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

Before you begin

You need the following information for restoring the External Key Manager (EKM) configuration.

- A copy of the /cfcard/kmip/servers.cfg file from another cluster node or the following information:
 - The KMIP server address.
 - The KMIP port.
- A copy of the /cfcard/kmip/certs/client.crt file from another cluster node or the client certificate.

- A copy of the `/cfcard/kmip/certs/client.key` file from another cluster node or the client key.
- A copy of the `/cfcard/kmip/certs/CA.pem` file from another cluster node or the KMIP server CA(s).

Steps

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

Show example boot menu

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

3. When prompted, confirm you have gathered the required information.

Show example prompt

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

4. When prompted, enter the client and server information.

Show prompt

```
Enter the client certificate (client.crt) file contents:
Enter the client key (client.key) file contents:
Enter the KMIP server CA(s) (CA.pem) file contents:
Enter the server configuration (servers.cfg) file contents:
```

Show example

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

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

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

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

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

After you enter the client and server information, the recovery process completes.

Show example

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

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

Show example prompt

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

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

6. Restore automatic giveback if you disabled it.

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

7. If AutoSupport is enabled, restore automatic case creation by entering the following command.

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

Return the failed boot media to NetApp - ASA C800

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

Chassis

Replace the chassis - ASA C800

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 - ASA C800

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

Before you begin

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

Make note of any faults presently on the system, such as LEDs on the system components.

Steps

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

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

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

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

6. Exit the cluster shell:

```
exit
```

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

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

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

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



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

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

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

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

Move and replace hardware - ASA C800

Move the power supplies, hard drives, and controller module from the impaired chassis to the new chassis, and swap out the impaired chassis with the new chassis of the same model as the impaired chassis.

Step 1: Remove the controller modules

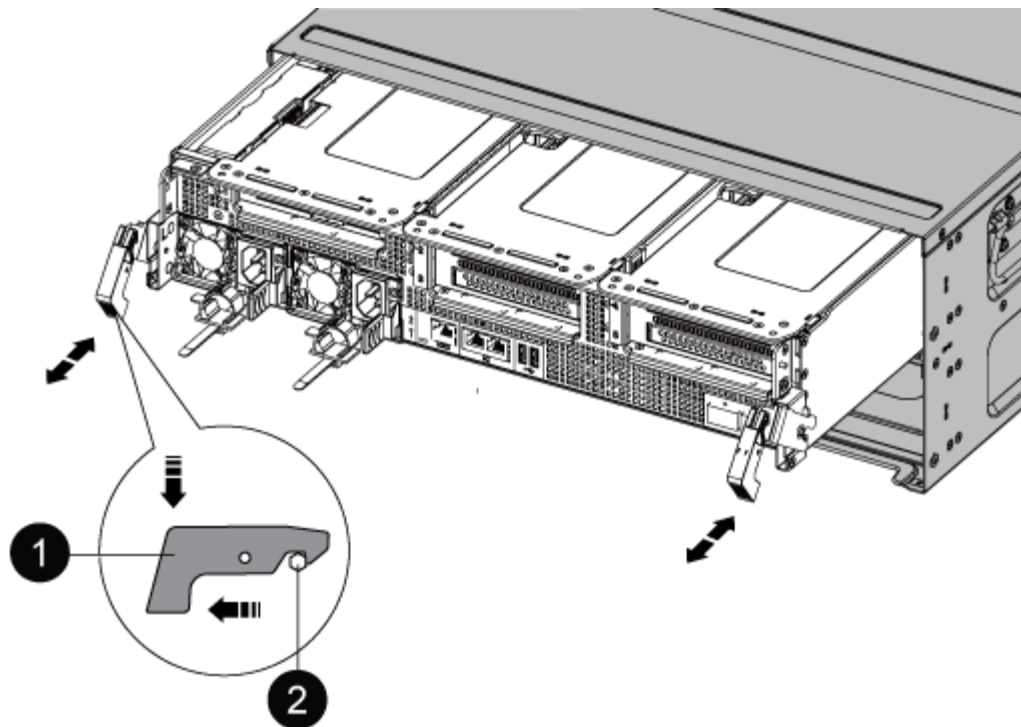
To replace the chassis, you must remove the controller modules from the old chassis.

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 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 latch
2	Locking pin

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 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.

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. Complete the reinstallation of the controller module:
 - a. 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.

- b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
- c. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. 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 by pressing `Ctrl-C`.
4. Repeat the preceding steps to install the second controller into the new chassis.

Complete the restoration and replacement process - ASA C800

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

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

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

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: Return the failed part to NetApp

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

Controller

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.
- 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.
- 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.



Do not downgrade the BIOS version of the *replacement* controller to match the partner controller or the old controller module.

Shut down the impaired controller - ASA C800

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <code>-halt true</code> parameter brings you to the LOADER prompt.</p>

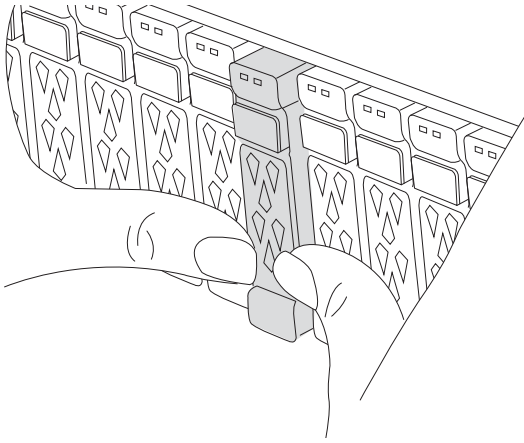
Replace the controller module hardware - ASA C800

To replace the controller, 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 the controller module or replace a component inside the controller module.

1. Ensure that all drives in the chassis are firmly seated against the midplane by using your thumbs to push each drive until you feel a positive stop.

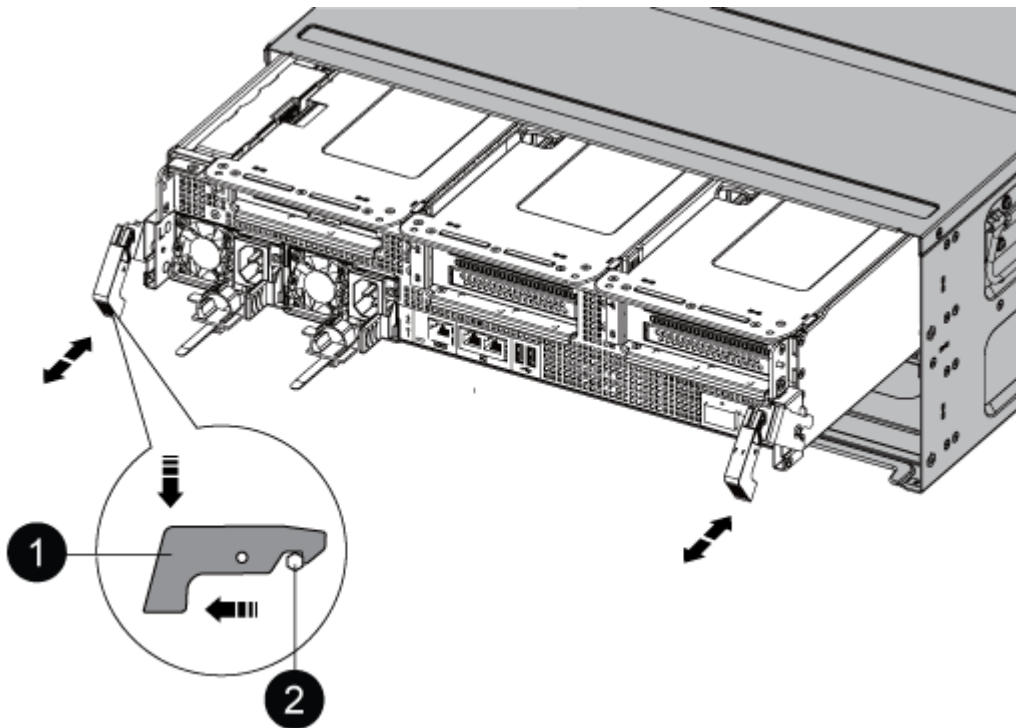


2. Go to the rear of the chassis. If you are not already grounded, properly ground yourself.
3. Unplug the controller module power supplies from the source.
4. Release the power cable retainers, and then unplug the cables from the power supplies.
5. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (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.

6. Remove the cable management device from the controller module and set it aside.
7. 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 latch
2	Locking pin

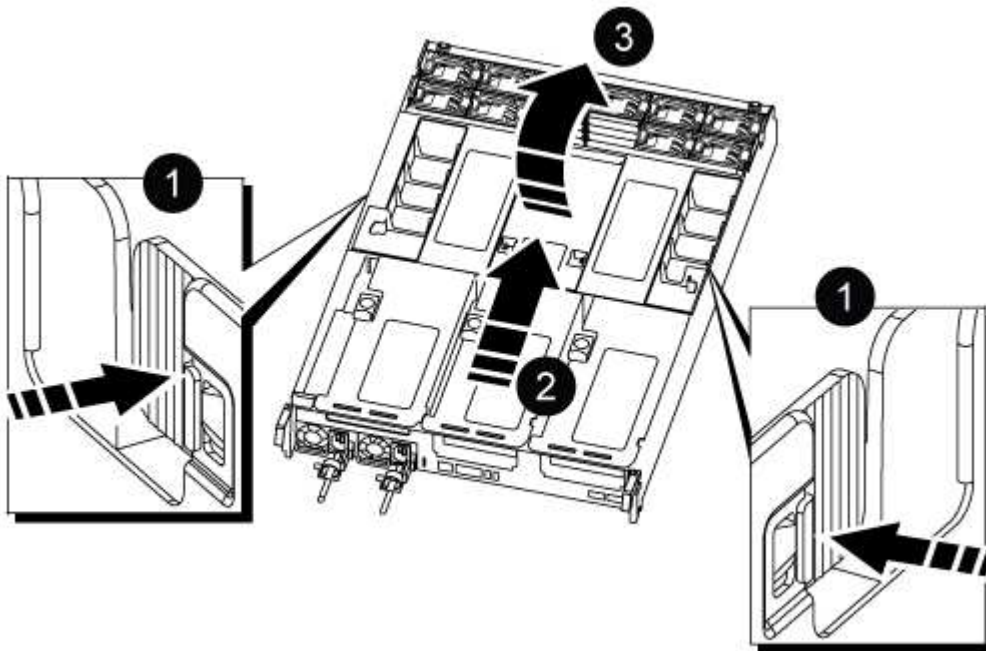
8. Slide the controller module out of the chassis and place it on a stable, flat surface.

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

9. Place the controller module on a stable, flat surface.

10. Open the controller module air duct:

- a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
- b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.



1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

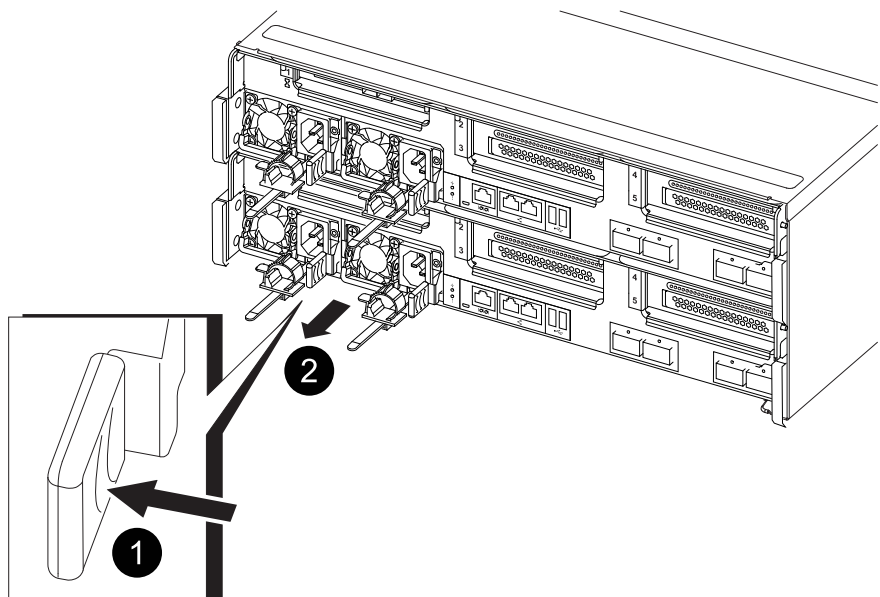
Step 2: Move the power supplies

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

1. 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

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.

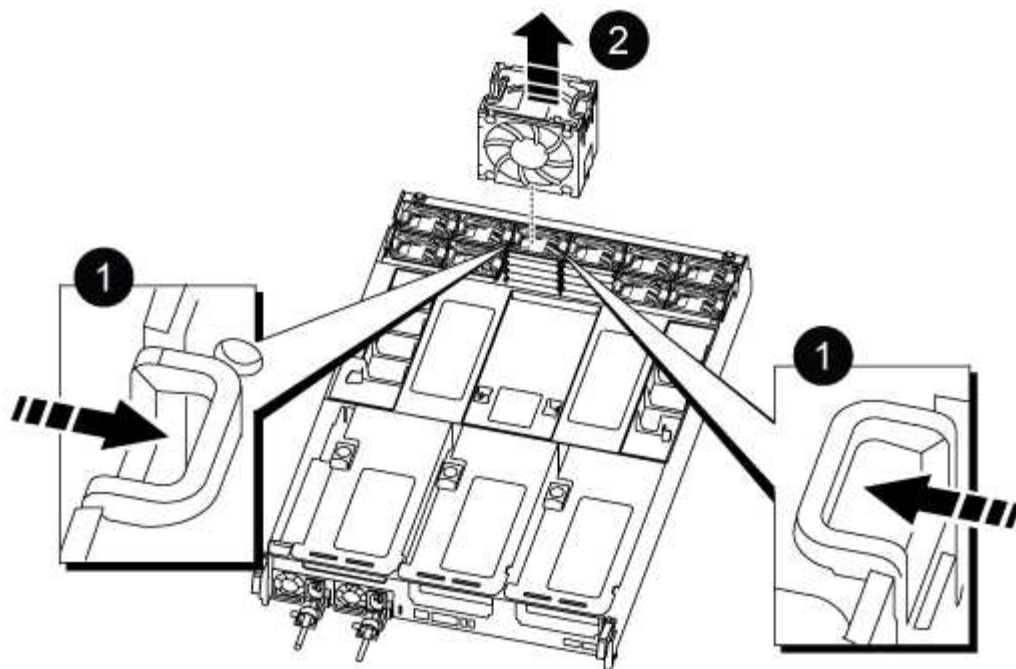


To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

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 locking tabs on the side of the fan module, and then lifting the fan module straight out of the controller module.



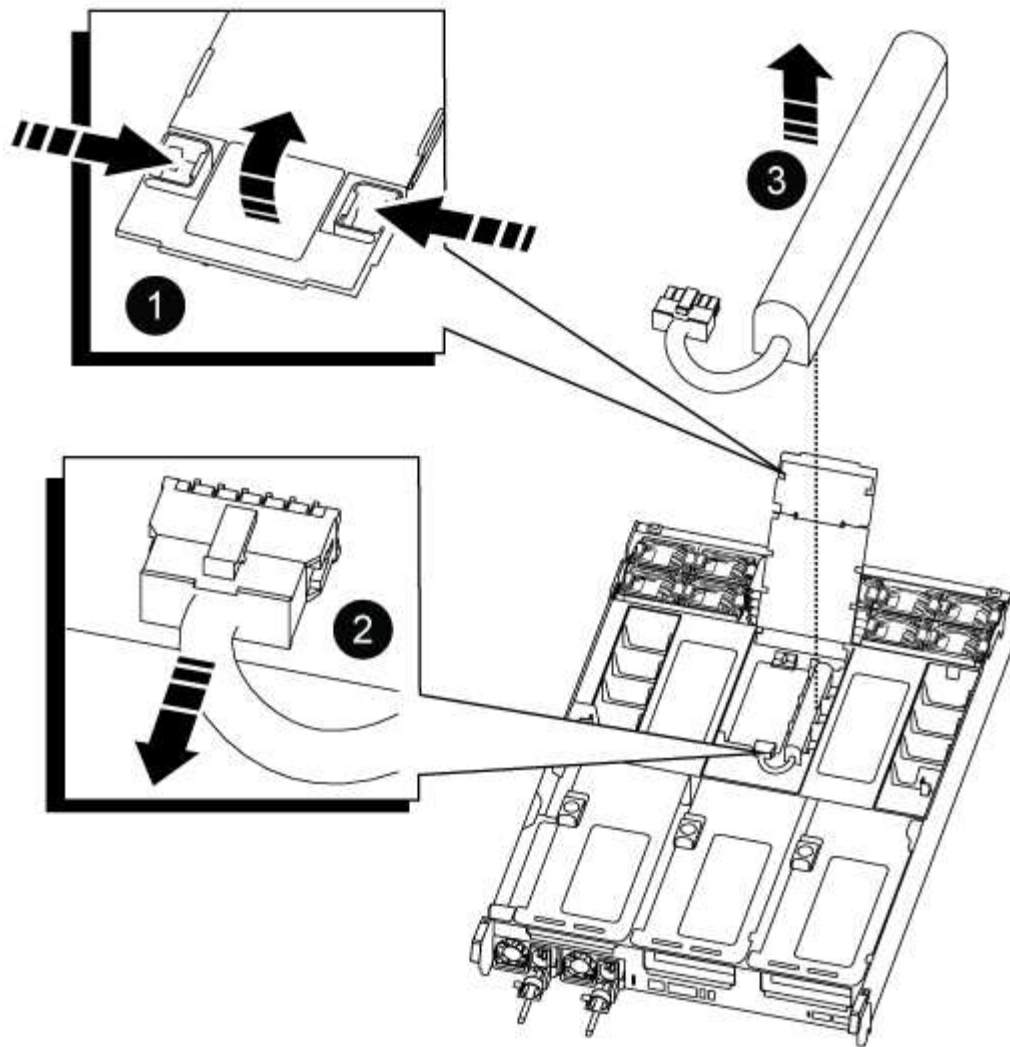
1	Fan locking tabs
2	Fan module

2. Move the fan module to the replacement controller module, and then install the fan module by aligning its edges with the opening in the controller module, and then sliding the fan module into the controller module until the locking latches click into place.
3. Repeat these steps for the remaining fan modules.

Step 4: Move the NVDIMM battery

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

1. Open the air duct cover and locate the NVDIMM battery in the riser.



1	Air duct riser
2	NVDIMM battery plug
3	NVDIMM battery pack

Attention: The NVDIMM battery control board LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

2. 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.
3. Grasp the battery and lift the battery out of the air duct and controller module.
4. Move the battery pack to the replacement controller module and then install it in the NVDIMM air duct:
 - a. Insert the battery pack into the slot and press firmly down on the battery pack to make sure that it is locked into place.
 - b. Plug the battery plug into the riser socket and make sure that the plug locks into place.

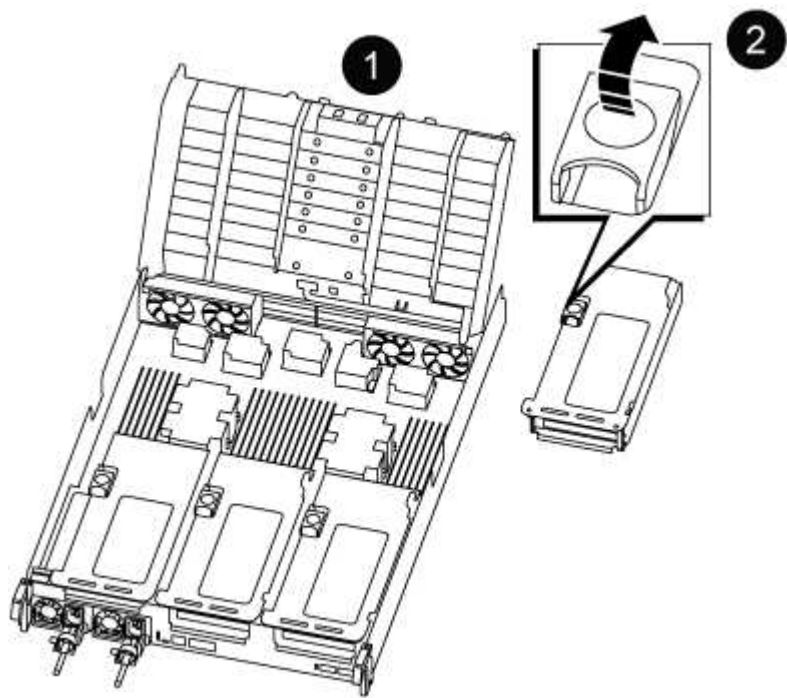
Step 5: Remove the PCIe risers

As part of the controller replacement process, you must remove the PCIe modules from the impaired controller module. You must install them into the same location in the replacement controller module once the NVDIMMS and DIMMs have moved to the replacement controller module.

- 1. Remove the PCIe riser from the 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 the fan modules.

The riser raises up slightly from the controller module.

- c. Lift the riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.



1	Air duct
2	Riser 1 (left riser), Riser 2 (middle riser), and 3 (right riser) locking latches

- 2. Repeat the preceding step for the remaining risers in the impaired controller module.
- 3. Repeat the above steps with the empty risers in the replacement controller and put them away.

Step 6: Move system DIMMs

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

- 1. 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.

2. 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.

3. Locate the slot where you are installing the DIMM.
4. 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.



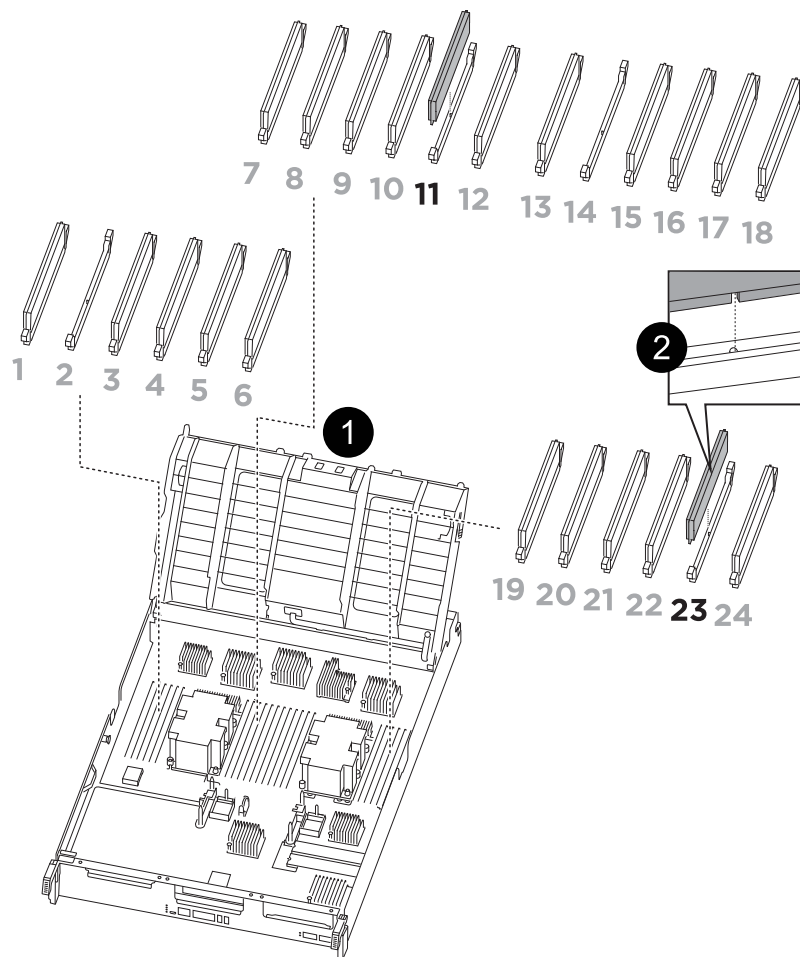
Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

5. 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.
6. Repeat these steps for the remaining DIMMs.

Step 7: Move the NVDIMMs

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

1. Locate the NVDIMMs on your controller module.



- NVDIMM: SLOTS 11 & 23

1	Air duct
2	NVDIMMs

2. Note the orientation of the NVDIMM in the socket so that you can insert the NVDIMM in the replacement controller module in the proper orientation.
3. 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.

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.

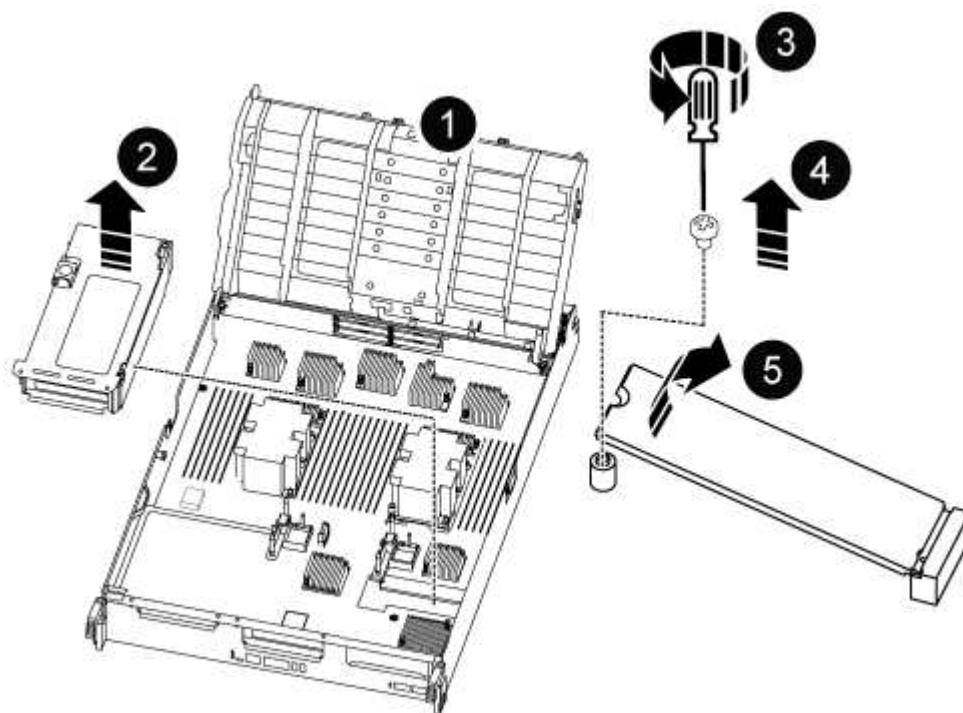
6. Push carefully, but firmly, on the top edge of the NVDIMM until the ejector tabs snap into place over the notches at the ends of the NVDIMM.
7. Repeat the preceding steps to move the other NVDIMM.

Step 8: Move the boot media

You must move the boot media device from the impaired controller and install it in the replacement controller.

The boot media is located under Riser 3.

1. Locate the boot media:



1	Air duct
2	Riser 3
3	Phillips #1 screwdriver
4	Boot media screw
5	Boot media

2. Remove the boot media from the controller module:
 - a. Using a #1 Phillips head screwdriver, remove the screw holding down the boot media and set the screw aside in a safe place.

- b. Grasping the sides of the boot media, gently rotate the boot media up, and then pull the boot media straight out of the socket and set it aside.
3. Move the boot media to the new controller module and install it:
 - a. Align the edges of the boot media with the socket housing, and then gently push it squarely into the socket.
 - b. Rotate the boot media down toward the motherboard.
 - c. Secure the boot media to the motherboard using the boot media screw.

Do not over-tighten the screw or you might damage the boot media.

Step 9: Install the PCIe risers

You install the PCIe risers in the replacement controller module after moving the DIMMs, NVDIMMs, and boot media.

1. Install the riser into the replacement controller module:
 - a. Align the lip of the riser with the underside of the controller module sheet metal.
 - b. Guide the riser along the pins in the controller module, and then lower the riser into the controller module.
 - c. Swing the locking latch down and click it into the locked position.

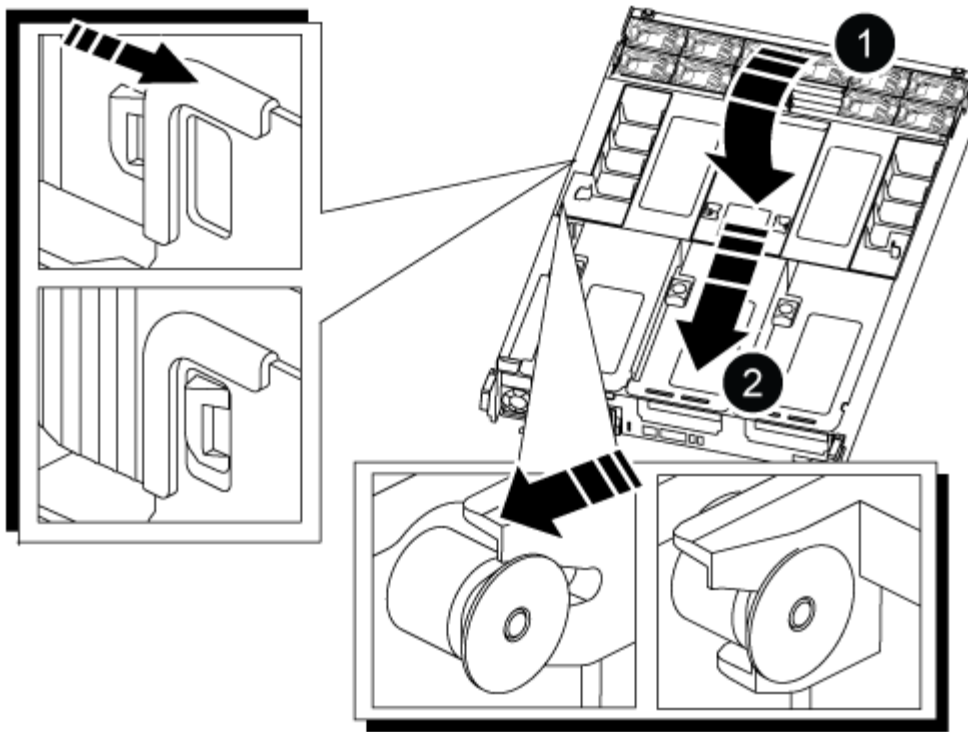
When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

- d. Reinsert any SFP or QSFP modules that were removed from the PCIe cards.
2. Repeat the preceding step for the remaining PCIe risers.

Step 10: 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.

1. If you have not already done so, close the air duct:
 - a. Swing the air duct all the way down to the controller module.
 - b. Slide the air duct toward the risers until the locking tabs click into place.
 - c. Inspect the air duct to make sure that it is properly seated and locked into place.



1	Locking tabs
2	Slide plunger

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 reinstallation of the controller module:

- a. 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.

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

5. Plug the system cables and transceiver modules into the controller module and reinstall the cable management device.

6. Plug the power cables into the power supplies and reinstall the power cable retainers.

The controller module begins to boot as soon as it is connected to power. Be prepared to interrupt the boot process.



If your system has DC power supplies, make sure the thumbscrews on the power supply cable are tight.

Restore and verify the system configuration - ASA C800

After completing the hardware replacement and booting to Maintenance mode, you verify the low-level system configuration of the replacement controller and reconfigure system settings as necessary.

Step 1: Set and verify system time

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

About this task

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

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

Steps

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

The date and time are based on the configured timezone.

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

The date and time are given in GMT.

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

The date and time are given in GMT.

Step 2: Verify and set the 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`

Recable the system and reassign disks - ASA C800

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

Step 1: Recable the system

Verify the controller module's storage and network connections.

Steps

1. 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: `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`
```

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

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

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

6. Give back the 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.

- b. After the giveback has been completed, confirm that the HA pair is healthy and that takeover is possible: `storage failover show`

The output from the `storage failover show` command should not include the System ID changed on partner message.

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

The disks belonging to the *replacement* 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
.
.
.
```

8. 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.

9. 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](#)

10. 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.

11. Verify that the expected volumes are present for each controller: `vol show -node node-name`
12. 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 - ASA C800

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.



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

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: 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 -vserver * -lif *`
2. Register the system serial number with NetApp Support.
 - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
 - If AutoSupport is not enabled, call [NetApp Support](#) to register the serial number.
3. Check the health of your cluster. See the [How to perform a cluster health check with a script in ONTAP](#) KB article for more information.
4. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.
5. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

Step 3: Return the failed part to NetApp

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

Replace a DIMM - ASA C800

You must replace a DIMM in the controller when your storage system encounters errors such as, excessive CECC (Correctable Error Correction Codes) errors that are based on Health Monitor alerts or uncorrectable ECC errors, typically caused by a single DIMM failure preventing the storage system from booting ONTAP.

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

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

Step 1: Shut down the impaired controller

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:
- a. Enter the following command from the console of the healthy controller:

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

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

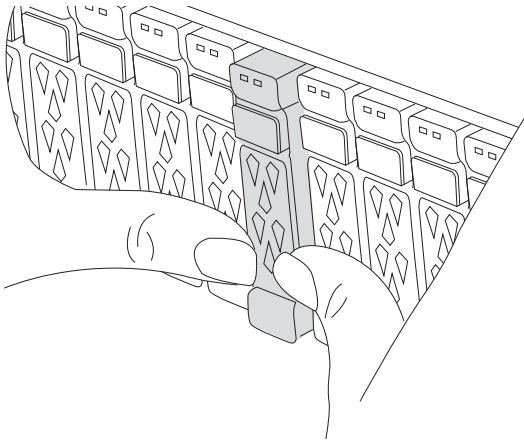
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	Take over or halt the impaired controller from the healthy controller: <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> The <code>-halt true</code> parameter brings you to the LOADER prompt.

Step 2: Remove the controller module

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

1. If you are not already grounded, properly ground yourself.
2. Ensure that all drives in the chassis are firmly seated against the midplane by using your thumbs to push each drive until you feel a positive stop.

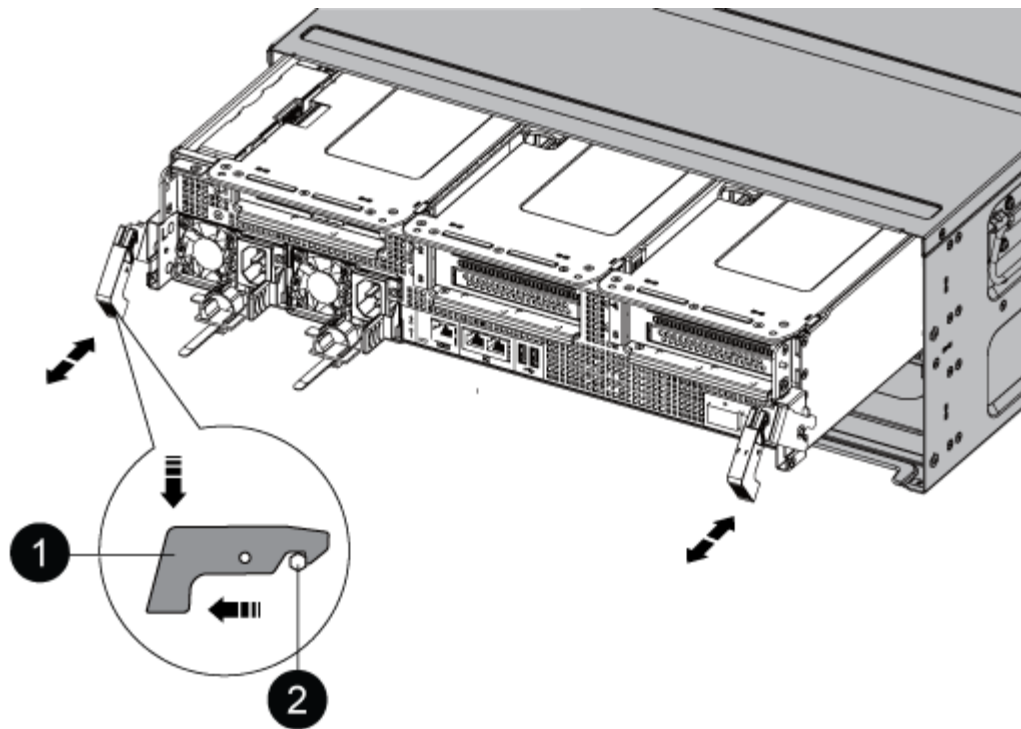


3. Unplug the controller module power supplies from the source.
4. Release the power cable retainers, and then unplug the cables from the power supplies.
5. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if 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.

6. Remove the cable management device from the controller module and set it aside.
7. 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.



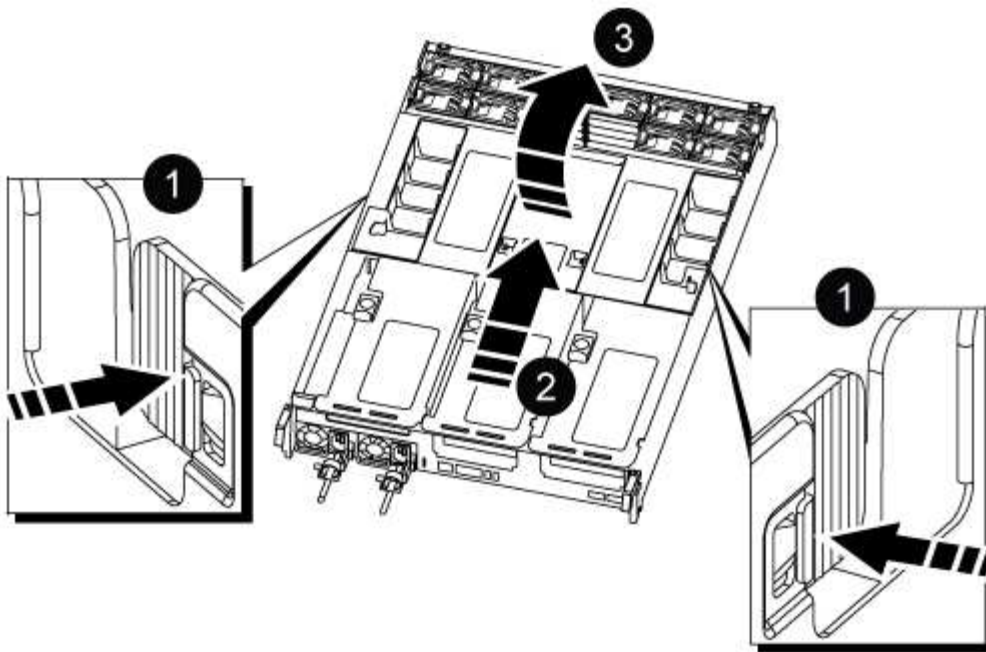
1	Locking latch
2	Locking pin

8. 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.

9. Place the controller module on a stable, flat surface, and then open the air duct:

- Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
- Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

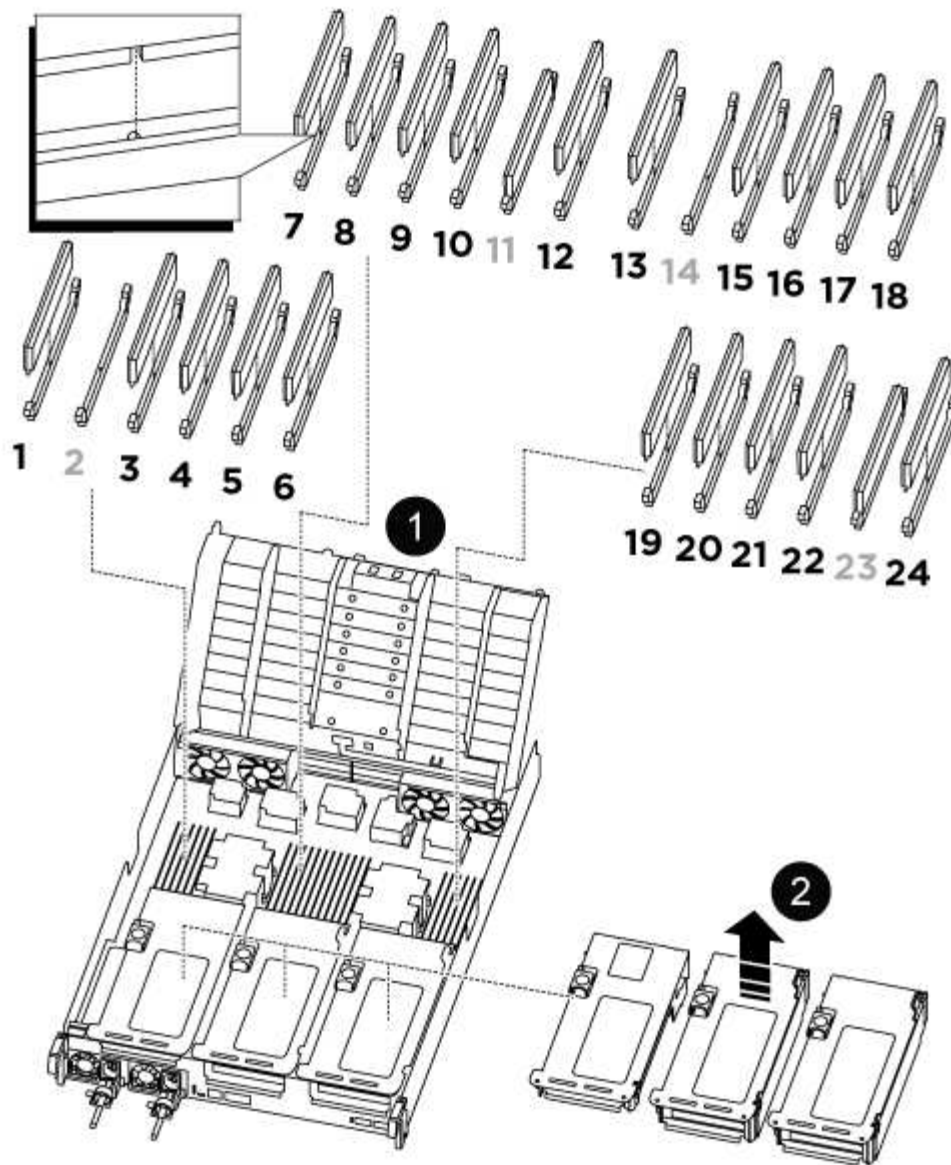


1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

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 and then replace it following the specific sequence of steps.

1. When removing a DIMM, unlock the locking latch on the applicable riser, and then remove the riser.



1	Air duct cover
2	Riser 1 and DIMM bank 1, and 3-6
Riser 2 and DIMM bank 7-10, 12-13, and 15-18	Riser 3 and DIMM 19 -22 and 24

Note: Slot 2 and 14 are left empty. Do not attempt to install DIMMs into these slots.

- Note the orientation of the DIMM in the socket so that you can insert the replacement DIMM in the proper orientation.
- 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.

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. 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.



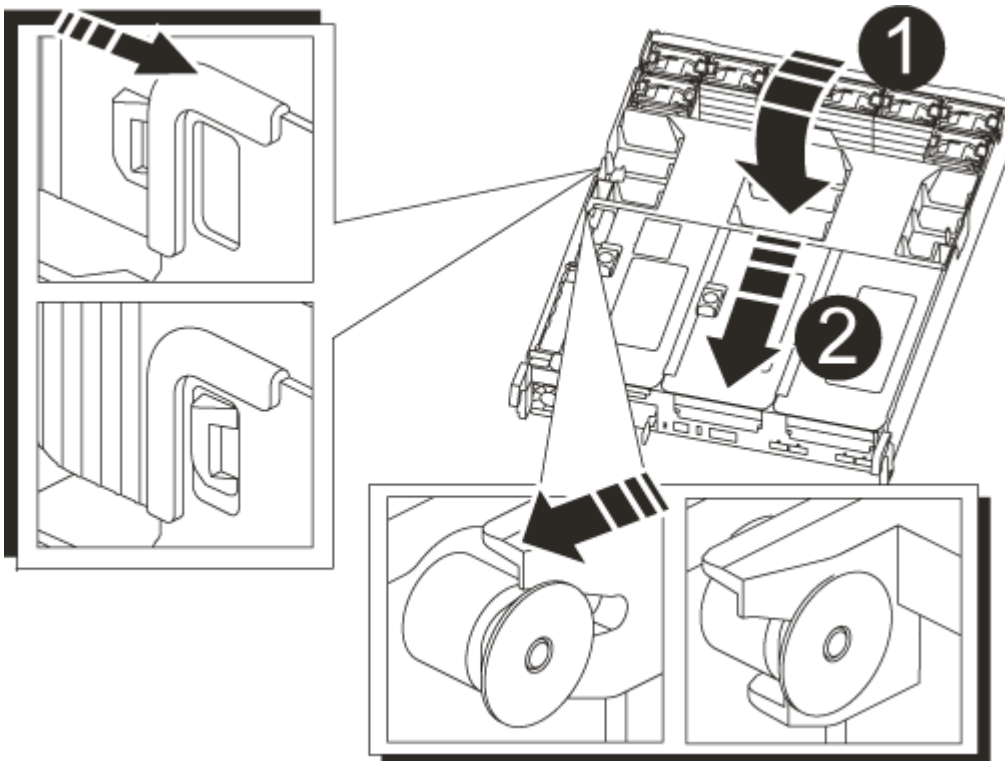
Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

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. Reinstall any risers that you removed from the controller module.
8. Close the air duct.

Step 4: Reinstall the controller module and booting the system

After you replace a FRU in the controller module, you must reinstall the controller module and reboot it.

1. If you have not already done so, close the air duct:
 - a. Swing the air duct all the way down to the controller module.
 - b. Slide the air duct toward the risers until the locking tabs click into place.
 - c. Inspect the air duct to make sure that it is properly seated and locked into place.



1	Locking tabs
2	Slide plunger

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:

- a. 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.

- b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
- c. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

- d. If you have not already done so, reinstall the cable management device.

Step 5: Return the failed part to NetApp

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

Replace SSD Drive or HDD Drive - ASA C800

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 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 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 drive depends on how the 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 a drive, you must wait one minute between the removal of the failed drive and the insertion of the replacement drive to allow the storage system to recognize the existence of the new drive.

Option 1: Replace SSD

Steps

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

- 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 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 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 automatic 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 node_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 reenale 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 [NetApp Support](#) 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 reenale 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 automatic drive assignment in Step 1, then, manually assign drive ownership and then reenale 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 - ASA C800

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

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

3. Take the impaired controller to the LOADER prompt:

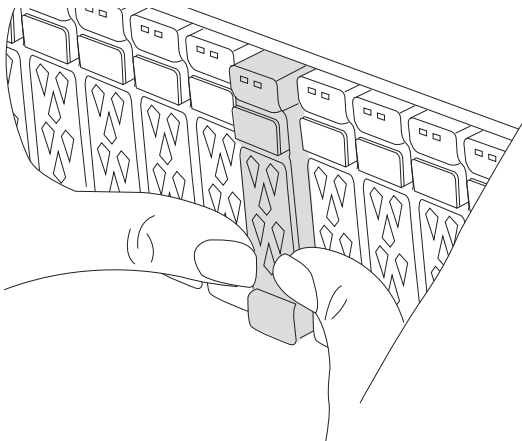
If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.

If the impaired controller is displaying...	Then...
Waiting for giveback...	Press Ctrl-C, and then respond <i>y</i> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

Step 2: Remove the controller module

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

1. If you are not already grounded, properly ground yourself.
2. Ensure that all drives in the chassis are firmly seated against the midplane by using your thumbs to push each drive until you feel a positive stop.

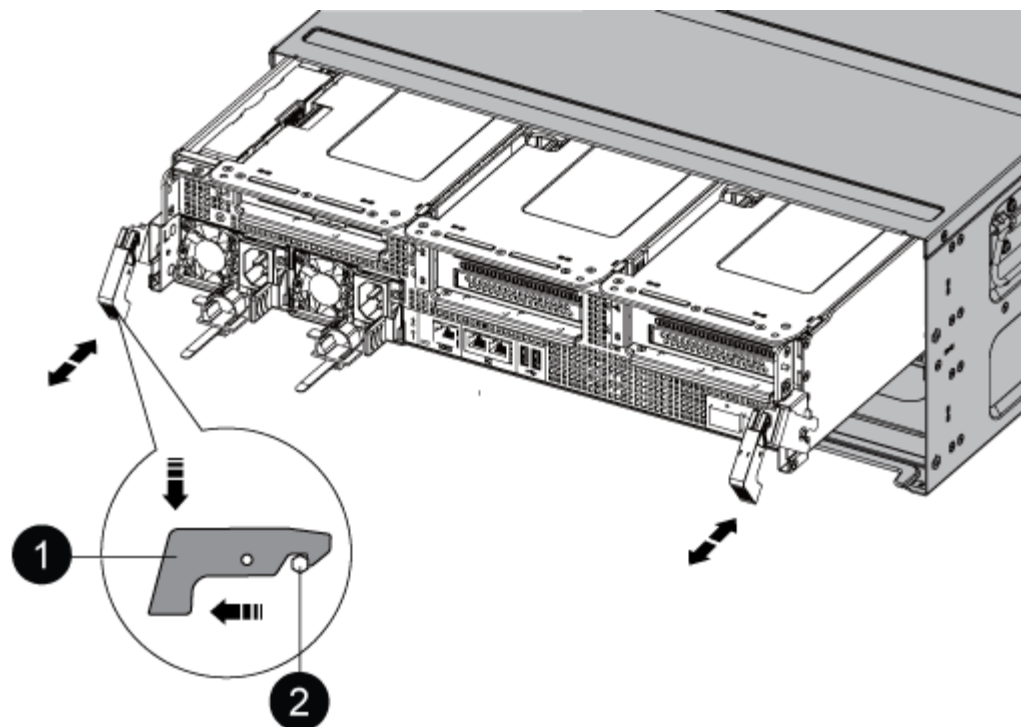


3. Unplug the controller module power supplies from the source.
4. Release the power cable retainers, and then unplug the cables from the power supplies.
5. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables from the controller module, 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.

6. Remove the cable management device from the controller module and set it aside.
7. 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 latch
2	Locking pin

8. Slide the controller module out of the chassis.

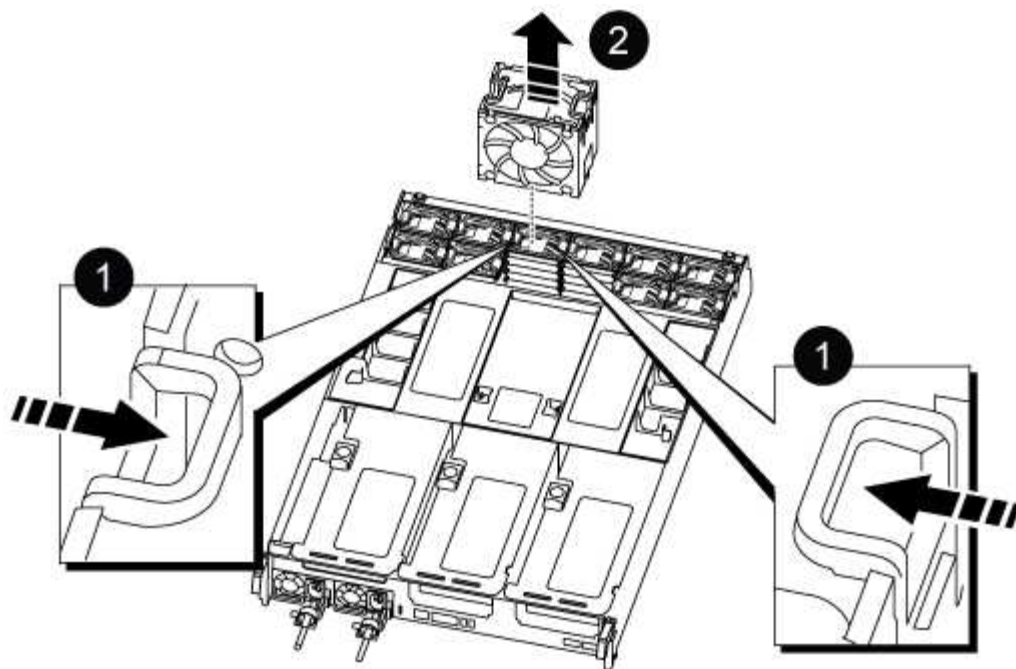
Make sure that you support the bottom of the controller module as you slide it out of the chassis.

9. Set the controller module aside in a safe place.

Step 3: Replace a fan

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

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 locking tabs on the side of the fan module, and then lifting the fan module straight out of the controller module.



1	Fan locking tabs
2	Fan module

- 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 until the locking latches click into place.

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.

- 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.

- Recable the system, as needed.
- Complete the reinstallation of the controller module:
 - 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.

- Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
- Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect

the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

- d. If you have not already done so, reinstall the cable management device.
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 -controller 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 and Replacements](#) page for further information.

Replace an NVDIMM - ASA C800

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

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

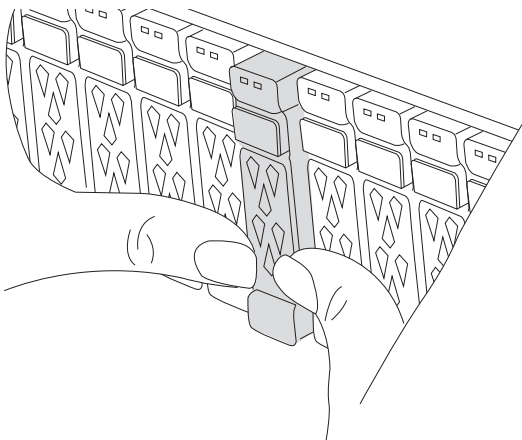
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <code>-halt true</code> parameter brings you to the LOADER prompt.</p>

Step 2: Remove the controller module

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

1. If you are not already grounded, properly ground yourself.
2. Ensure that all drives in the chassis are firmly seated against the midplane by using your thumbs to push each drive until you feel a positive stop.



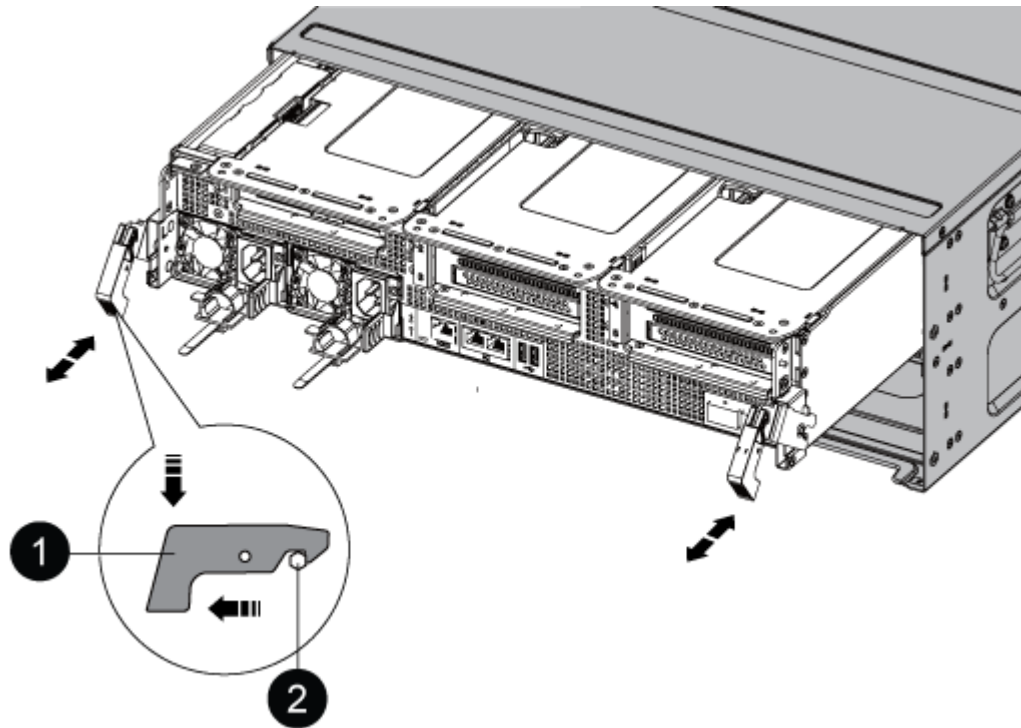
3. Unplug the controller module power supplies from the source.
4. Release the power cable retainers, and then unplug the cables from the power supplies.
5. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if 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.

6. Remove the cable management device from the controller module and set it aside.
7. 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.

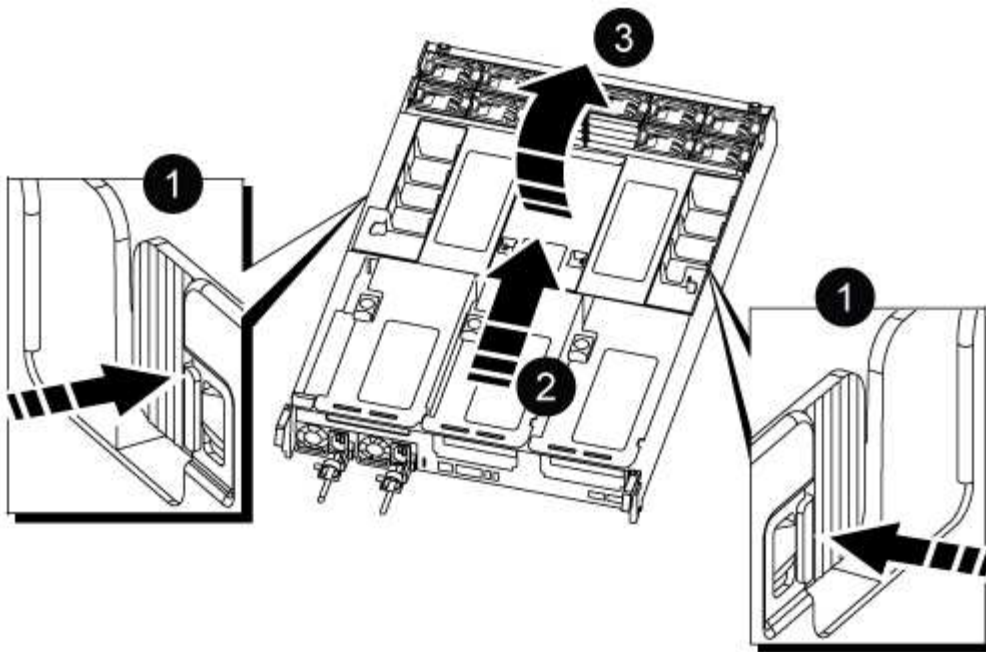


1	Locking latch
2	Locking pin

8. 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.

9. Place the controller module on a stable, flat surface, and then open the air duct:
 - a. Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
 - b. Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.

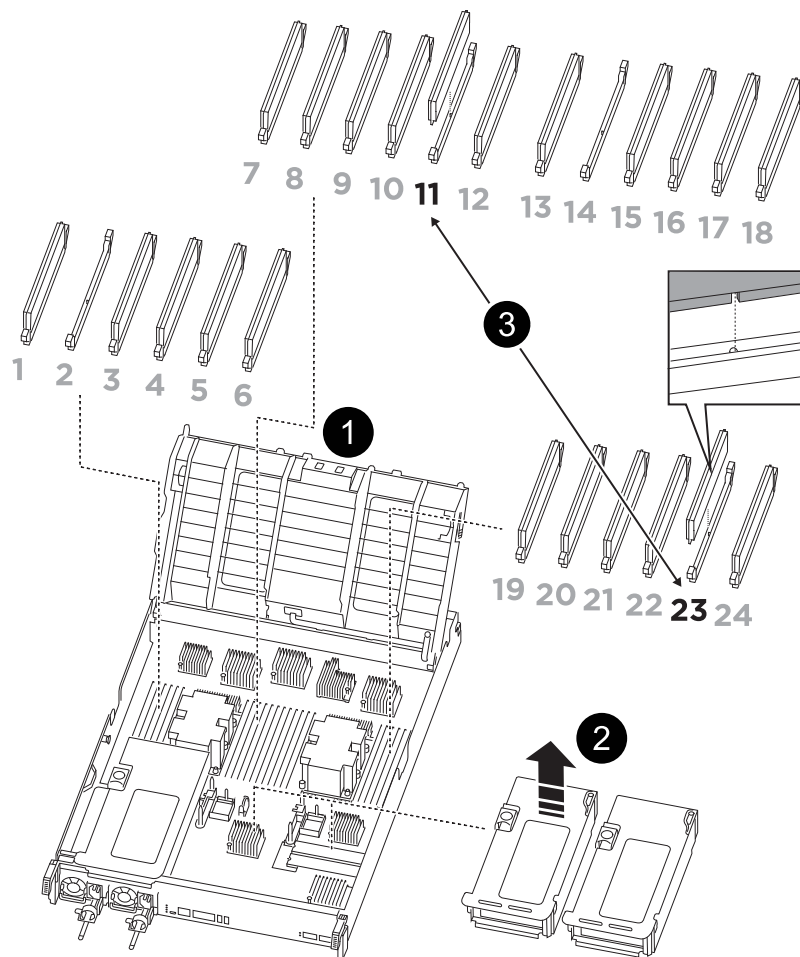


1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

Step 3: Replace the NVDIMM

To replace the NVDIMM, you must locate it in the controller module using the NVDIMM map label on top of the air duct, and then replace it following the specific sequence of steps.

1. If you are removing or moving an NVDIMM, unlock the locking latch on the riser, and then remove the applicable riser.



1	Air duct cover
2	Riser 2
3	NVDIMM in slots 11 and 23

- Note the orientation of the NVDIMM in the socket so that you can insert the NVDIMM in the replacement controller module in the proper orientation.
- 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.


- 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.

- Locate the slot where you are installing the NVDIMM.

6. 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.

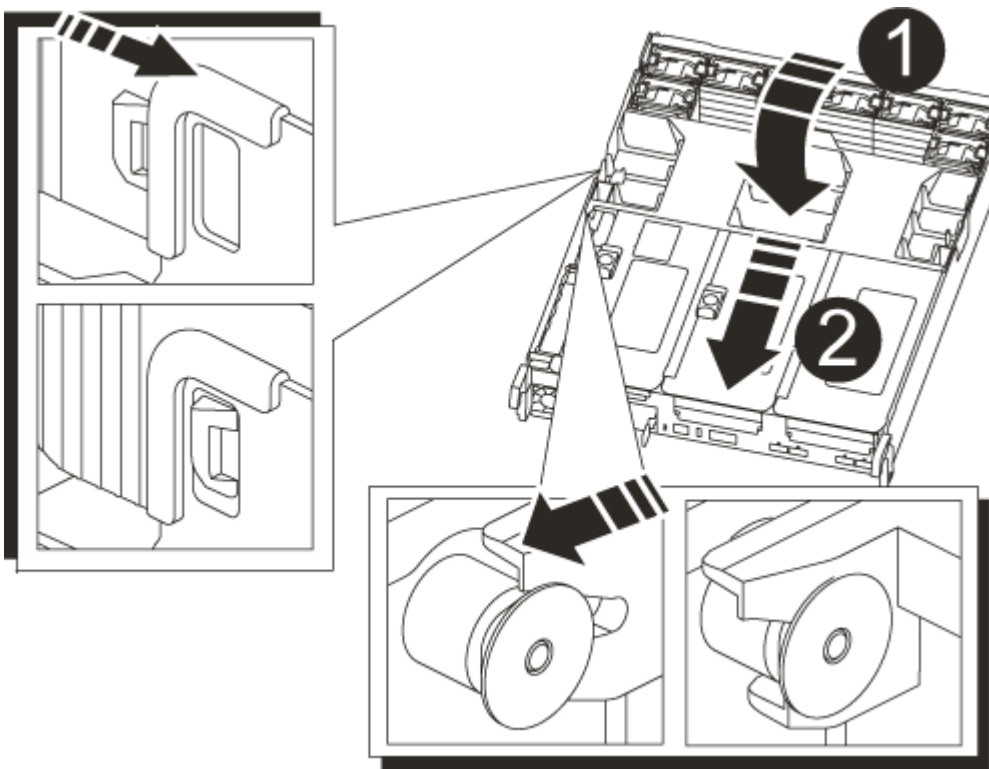
 Visually inspect the NVDIMM to verify that it is evenly aligned and fully inserted into the slot.



- 7. 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.
- 8. Reinstall any risers that you removed from the controller module.
- 9. Close the air duct.

Step 4: Reinstall the controller module and booting the system

After you replace a FRU in the controller module, you must reinstall the controller module and reboot it.

- 1. If you have not already done so, close the air duct:
 - a. Swing the air duct all the way down to the controller module.
 - b. Slide the air duct toward the risers until the locking tabs click into place.
 - c. Inspect the air duct to make sure that it is properly seated and locked into place.



	Locking tabs
	Slide plunger

- 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:

- a. 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.

- b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
- c. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

- d. If you have not already done so, reinstall the cable management device.

Step 4: Return the failed part to NetApp

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

Replace the NVDIMM battery - ASA C800

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

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

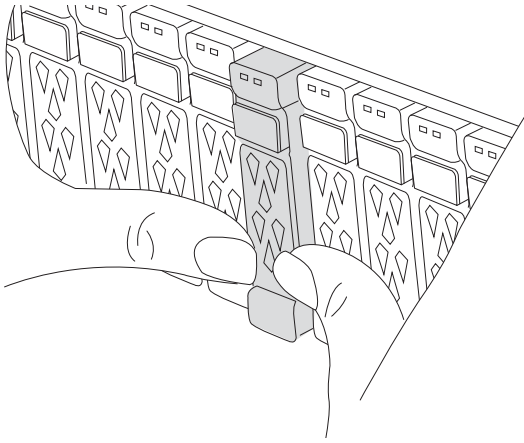
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

Step 2: Remove the controller module

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

1. If you are not already grounded, properly ground yourself.
2. Ensure that all drives in the chassis are firmly seated against the midplane by using your thumbs to push each drive until you feel a positive stop.

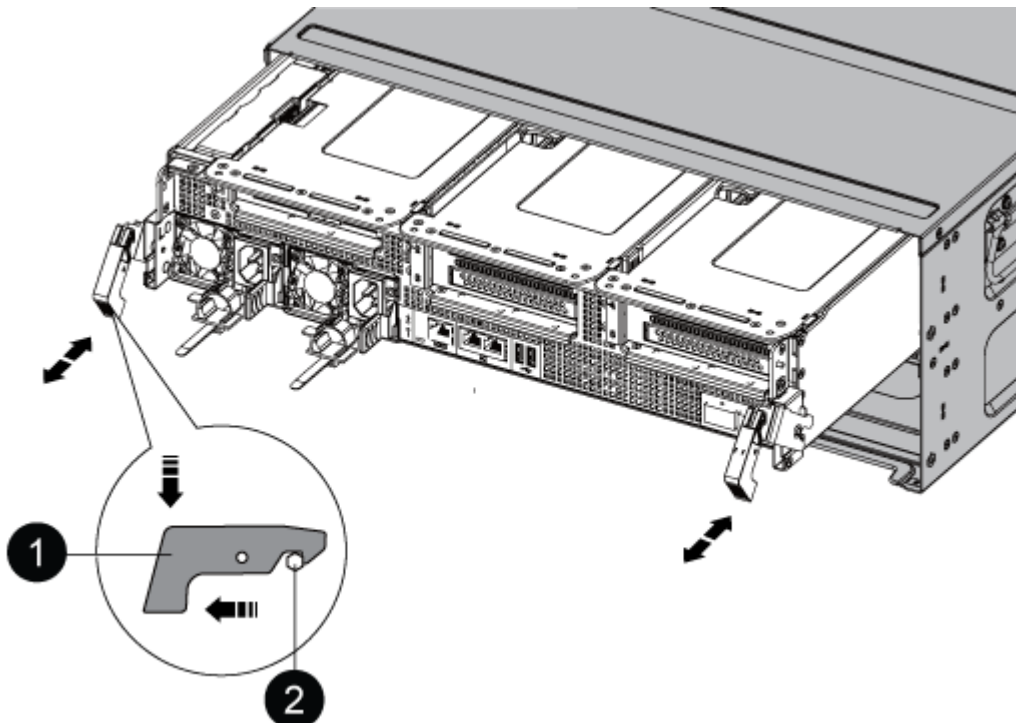


3. Unplug the controller module power supplies from the source.
4. Release the power cable retainers, and then unplug the cables from the power supplies.
5. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if needed) from the controller module, keeping track of where the cables were connected. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables 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.

6. Remove the cable management device from the controller module and set it aside.
7. 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 latch
2	Locking pin

8. Slide the controller module out of the chassis.

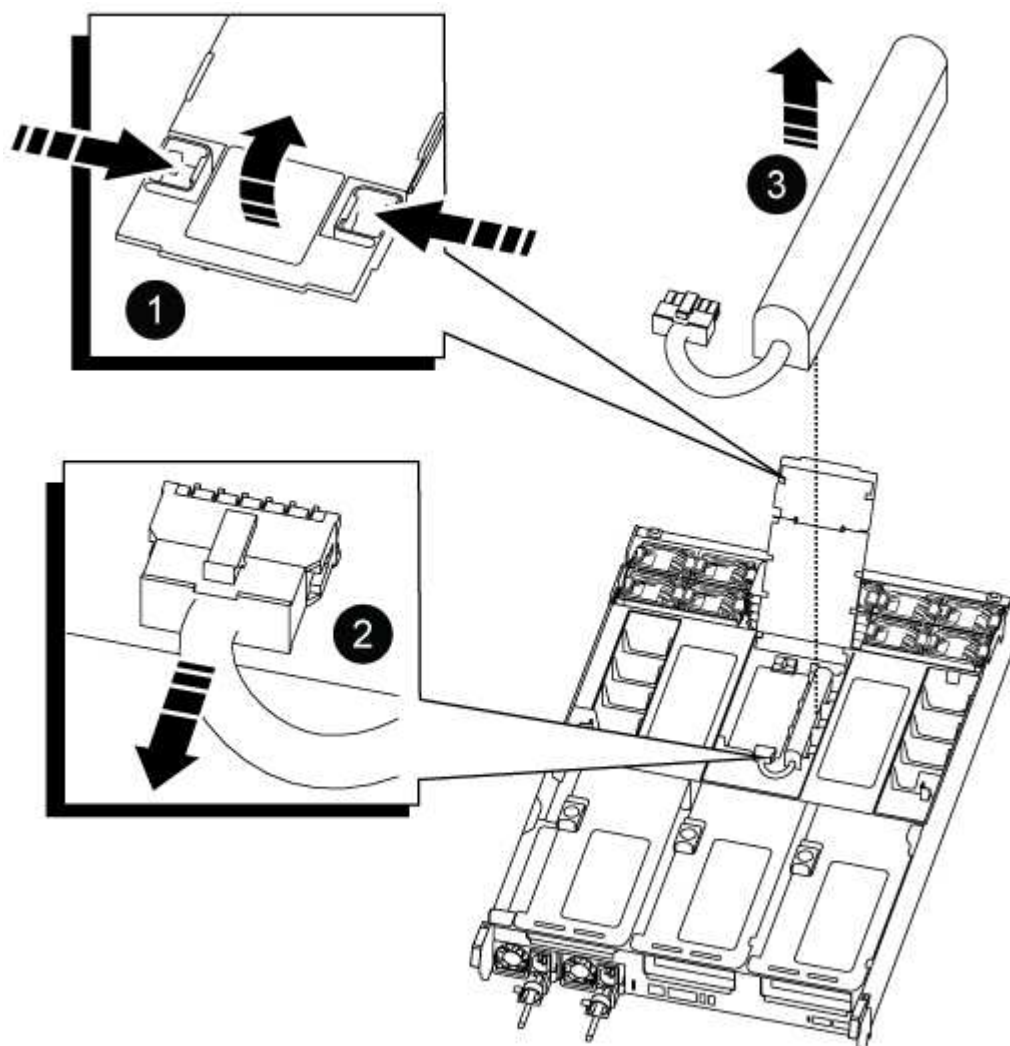
Make sure that you support the bottom of the controller module as you slide it out of the chassis.

9. Set the controller module aside in a safe place.

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.

1. Open the air duct cover and locate the NVDIMM battery in the riser.



1	Air duct riser
---	----------------

2	NVDIMM battery plug
3	NVDIMM battery pack

Attention: The NVDIMM battery control board LED blinks while destaging contents to the flash memory when you halt the system. After the destage is complete, the LED turns off.

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 lift the battery out of the air duct and controller module, and then set it aside.
3. Remove the replacement battery from its package.
4. Install the replacement battery pack in the NVDIMM air duct:
 - a. Insert the battery pack into the slot and press firmly down on the battery pack to make sure that it is locked into place.
 - b. Plug the battery plug into the riser socket and make sure that the plug locks into place.
5. Close the NVDIMM air duct.

Make sure that the plug locks into the socket.

Step 4: Reinstall the controller module and booting the system

After you replace a FRU in the controller module, you must reinstall the controller module and reboot 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:
 - a. 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.

- b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
 - c. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot

process.

- d. If you have not already done so, reinstall the cable management device.

Step 5: Return the failed part to NetApp

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

Replace a PCIe card - ASA C800

To replace a PCIe card, you must disconnect the cables from the cards, remove the SFP and QSFP modules from the cards before removing the riser, reinstall the riser, and then reinstall the SFP and QSFP modules before cabling 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

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

About this task

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

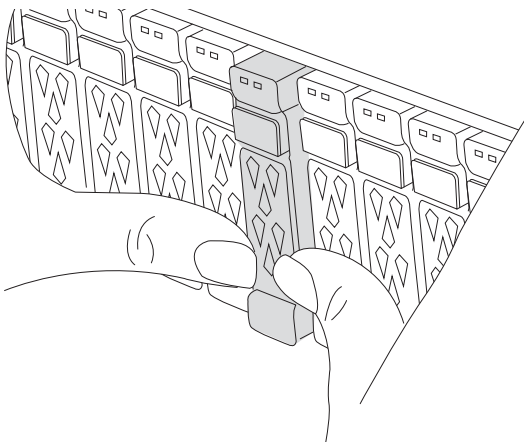
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <i>y</i> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

Step 2: Remove the controller module

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

1. If you are not already grounded, properly ground yourself.
2. Ensure that all drives in the chassis are firmly seated against the midplane by using your thumbs to push each drive until you feel a positive stop.

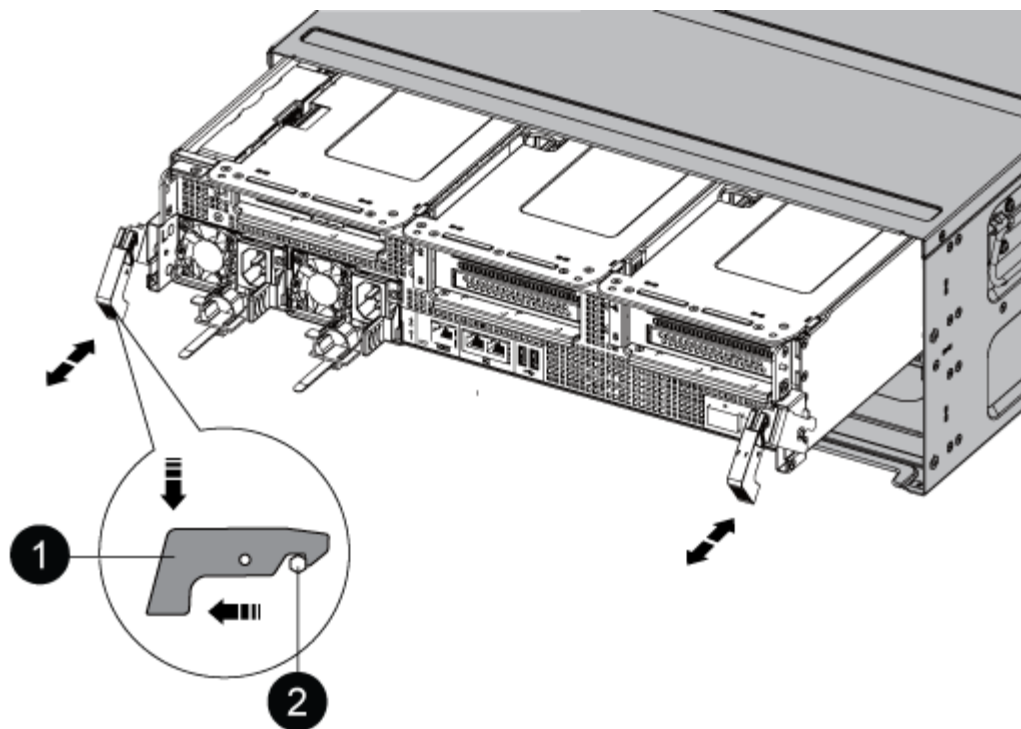


3. Unplug the controller module power supplies from the source.
4. Release the power cable retainers, and then unplug the cables from the power supplies.
5. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if 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.

6. Remove the cable management device from the controller module and set it aside.
7. 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.



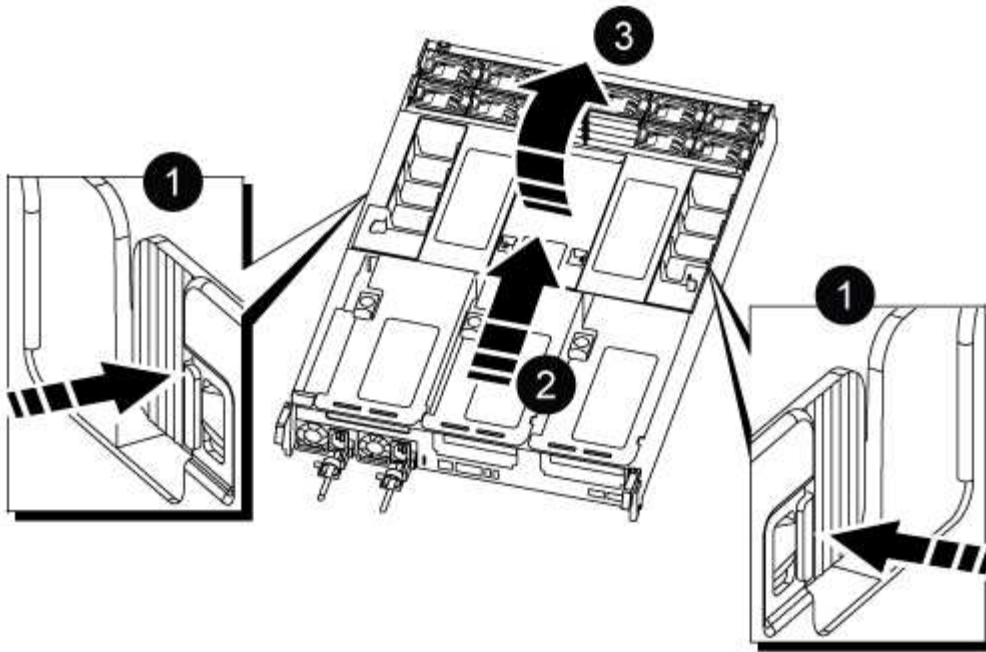
1	Locking latch
2	Locking pin

8. 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.

9. Place the controller module on a stable, flat surface, and then open the air duct:

- Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
- Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.



1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

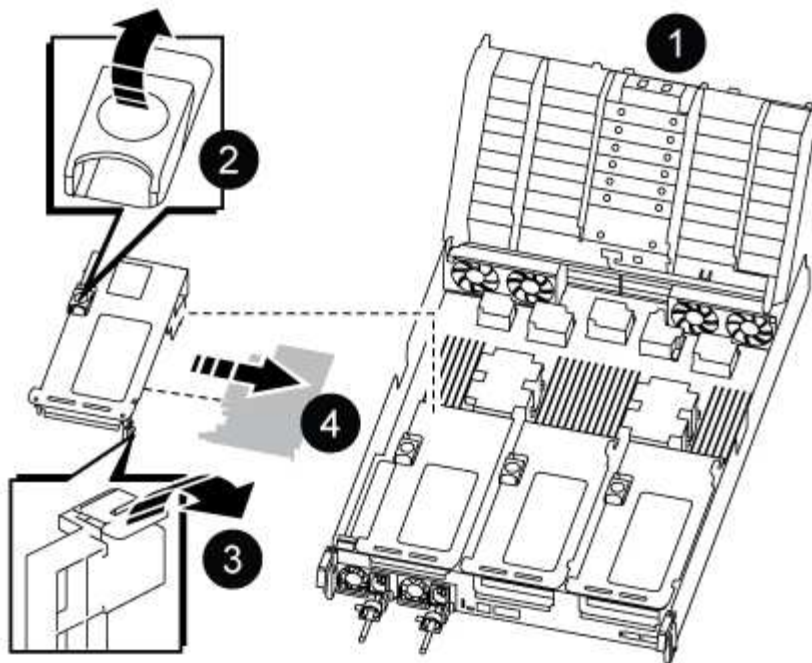
Step 3: Replace a PCIe card

To replace a PCIe card, you must remove the cabling and any QSFPs and SFPs from the ports on the PCIe cards in the target riser, remove the riser from the controller module, remove and replace the PCIe card, reinstall the riser and any QSFPs and SFPs onto the ports, and cable the ports.

1. Determine if the card you are replacing is from Riser 1 or if it is from Riser 2 or 3.
 - If you are replacing the 100GbE PCIe card in Riser 1, use Steps 2 - 3 and Steps 6 - 7.
 - If you are replacing a PCIe card from Riser 2 or 3, use Steps 4 through 7.
2. Remove Riser 1 from the controller module:
 - a. Remove the QSFP modules that might be in the PCIe card.
 - b. Rotate the riser locking latch on the left side of the riser up and toward the fan modules.

The riser raises up slightly from the controller module.

- c. Lift the riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.



1	Air duct
2	Riser locking latch
3	Card locking bracket
4	Riser 1 (left riser) with 100GbE PCIe card in slot 1.

3. Remove the PCIe card from Riser 1:

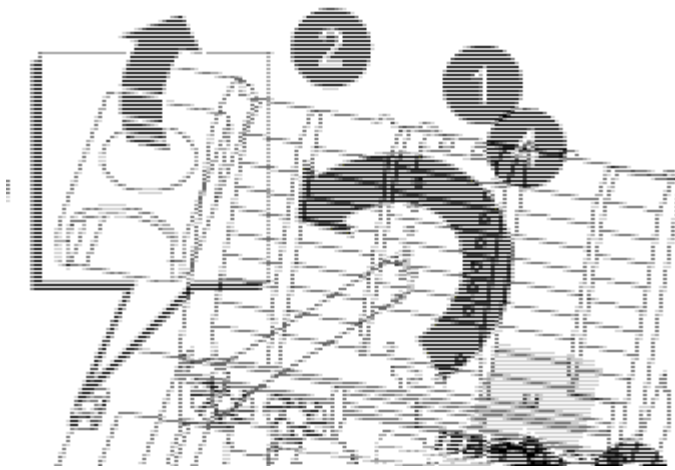
- a. Turn the riser so that you can access the PCIe card.
- b. Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.
- c. Remove the PCIe card from the riser.

4. Remove the PCIe riser from the 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 the fan modules.

The riser raises up slightly from the controller module.

- c. Lift the riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.



1	Air duct
2	Riser 2 (middle riser) or 3 (right riser) locking latch
3	Card locking bracket
4	Side panel on riser 2 or 3
5	PCIe cards in riser 2 or 3

5. Remove the PCIe card from the riser:

- Turn the riser so that you can access the PCIe cards.
- Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.
- Swing the side panel off the riser.
- Remove the PCIe card from the riser.

6. Install the PCIe card into the same slot in the riser:

- Align the card with the card socket in the riser, and then slide it squarely into the socket in the riser.



Make sure that the card is completely and squarely seated into the riser socket.

- For Riser 2 or 3, close the side panel.
- Swing the locking latch into place until it clicks into the locked position.

7. Install the riser into the controller module:

- Align the lip of the riser with the underside of the controller module sheet metal.
- Guide the riser along the pins in the controller module, and then lower the riser into the controller module.
- Swing the locking latch down and click it into the locked position.

When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the

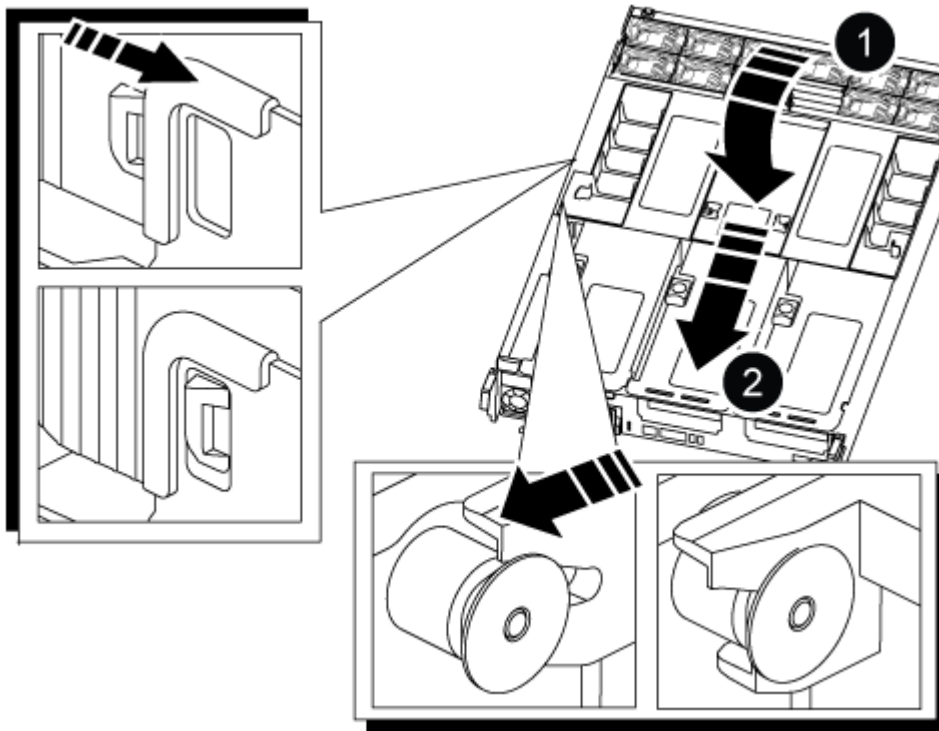
controller module.

- d. Reinsert any SFP modules that were removed from the PCIe cards.

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. If you have not already done so, close the air duct:
 - a. Swing the air duct all the way down to the controller module.
 - b. Slide the air duct toward the risers until the locking tabs click into place.
 - c. Inspect the air duct to make sure that it is properly seated and locked into place.



1	Locking tabs
2	Slide plunger

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 reinstallation of the controller module:

- a. 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.

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

5. Plug the system cables and transceiver modules into the controller module and reinstall the cable management device.

6. Plug the power cables into the power supplies and reinstall the power cable retainers.

The controller module begins to boot as soon as it is connected to power. Be prepared to interrupt the boot process.



If your system has DC power supplies, make sure the thumbscrews on the power supply cable are tight.

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

8. 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 and Replacements](#) page for further information.

Replace a power supply - ASA C800

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 it to the power source.

The power supplies are redundant and hot-swappable.

About this task

This procedure is written for replacing one PSU at a time.



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



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

Use the appropriate procedure for your type of PSU: AC or DC.

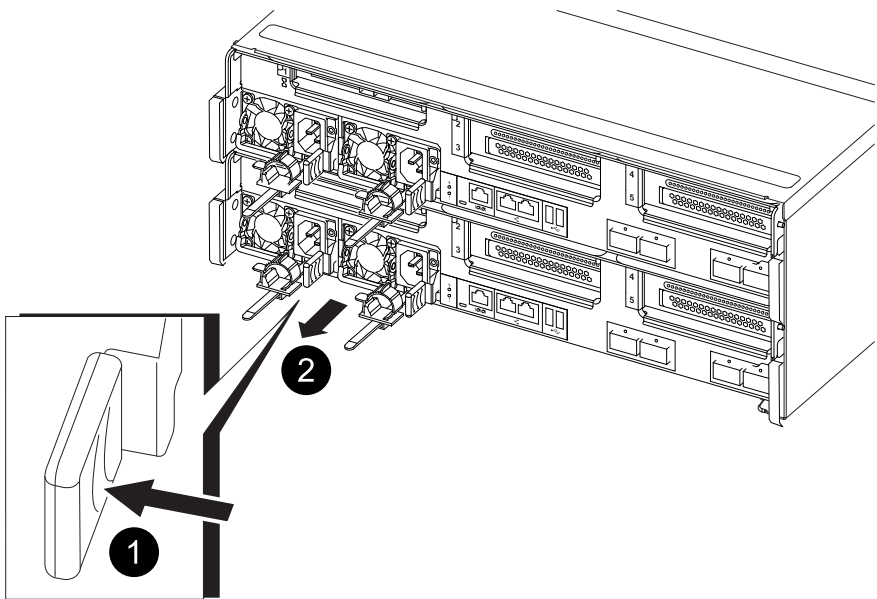
Option 1: Replace an AC PSU

To replace an AC PSU, complete the following steps.

1. If you are not already grounded, properly ground yourself.
2. Identify the PSU you want to replace, based on console error messages or through the red Fault LED on the PSU.
3. Disconnect the PSU:
 - a. Open the power cable retainer, and then unplug the power cable from the PSU.
 - b. Unplug the power cable from the power source.
4. Remove the PSU by rotating the handle up, press the locking tab, and then pull PSU out of the controller module.



The PSU 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 PSU locking tab
2	Power supply

5. Install the replacement PSU in the controller module:
 - a. Using both hands, support and align the edges of the replacement PSU with the opening in the controller module.
 - b. Gently push the PSU 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 PSU into the system.

6. Reconnect the PSU cabling:

- a. Reconnect the power cable to the PSU and the power source.
- b. Secure the power cable to the PSU using the power cable retainer.

Once power is restored to the PSU, 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 and Replacements](#) page for further information.

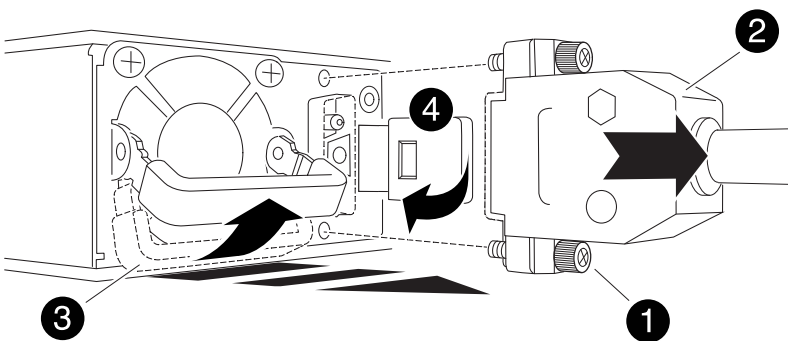
Option 2: Replace a DC PSU

To replace a DC PSU, complete the following steps.

1. If you are not already grounded, properly ground yourself.
2. Identify the PSU you want to replace, based on console error messages or through the red Fault LED on the PSU.
3. Disconnect the PSU:
 - a. Unscrew the D-SUB DC cable connector using the thumb screws on the plug.
 - b. Unplug the cable from the PSU and set it aside.
4. Remove the PSU by rotating the handle up, press the locking tab, and then pull the PSU out of the controller module.



The PSU 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	Thumb screws
2	D-SUB DC power PSU cable connector
3	Power supply handle

5. Install the replacement PSU in the controller module:

- a. Using both hands, support and align the edges of the replacement PSU with the opening in the controller module.
- b. Gently push the PSU 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 PSU into the system.

6. Reconnect the D-SUB DC power cable:

- a. Plug the power cable connector into the PSU.
- b. Secure the power cable to the PSU with the thumbscrews.

Once power is restored to the PSU, 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 and Replacements](#) page for further information.

Replace the real-time clock battery - ASA C800

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

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

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

Steps

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

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

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

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

2. Disable automatic giveback:

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

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

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

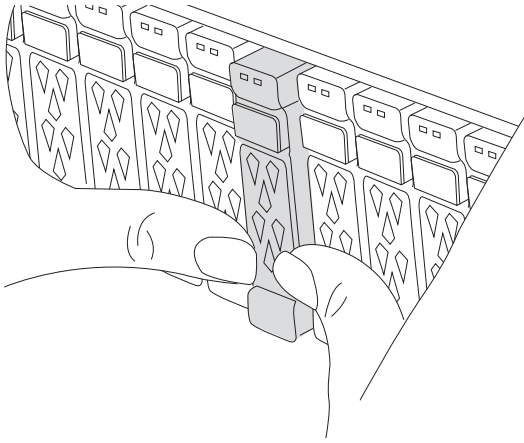
3. Take the impaired controller to the LOADER prompt:

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt	<p>Take over or halt the impaired controller from the healthy controller:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>The <i>-halt true</i> parameter brings you to the LOADER prompt.</p>

Step 2: Remove the controller module

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

1. If you are not already grounded, properly ground yourself.
2. Ensure that all drives in the chassis are firmly seated against the midplane by using your thumbs to push each drive until you feel a positive stop.

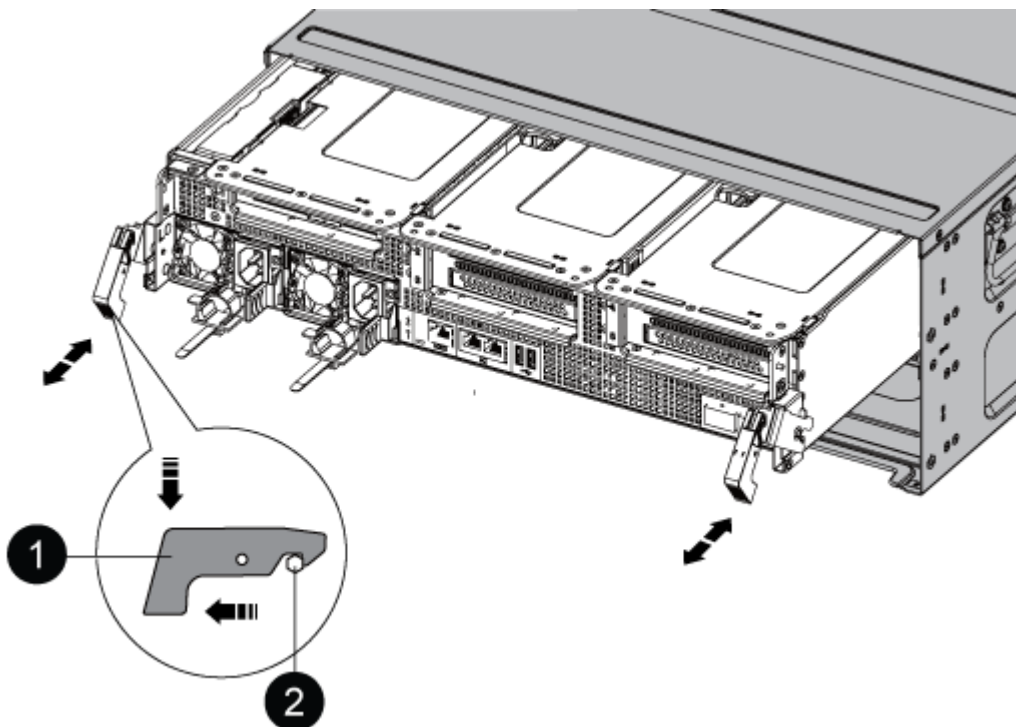


3. Unplug the controller module power supplies from the source.
4. Release the power cable retainers, and then unplug the cables from the power supplies.
5. Loosen the hook and loop strap binding the cables to the cable management device, and then unplug the system cables and SFP and QSFP modules (if 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.

6. Remove the cable management device from the controller module and set it aside.
7. 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.

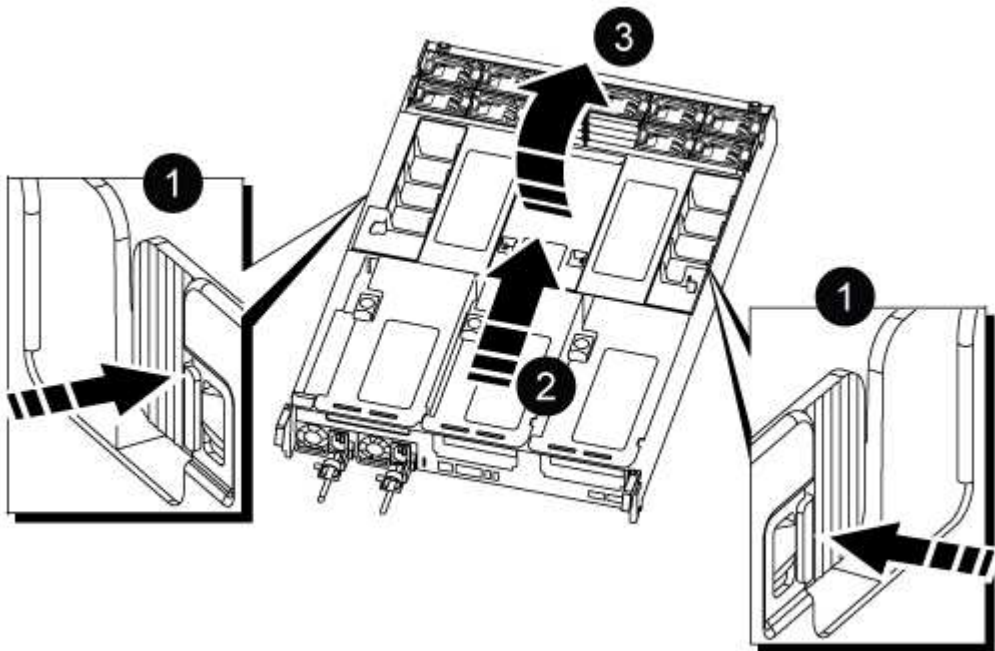


1	Locking latch
2	Locking pin

1. 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 on a stable, flat surface, and then open the air duct:
- Press in the locking tabs on the sides of the air duct toward the middle of the controller module.
 - Slide the air duct toward the fan modules, and then rotate it upward to its completely open position.



1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

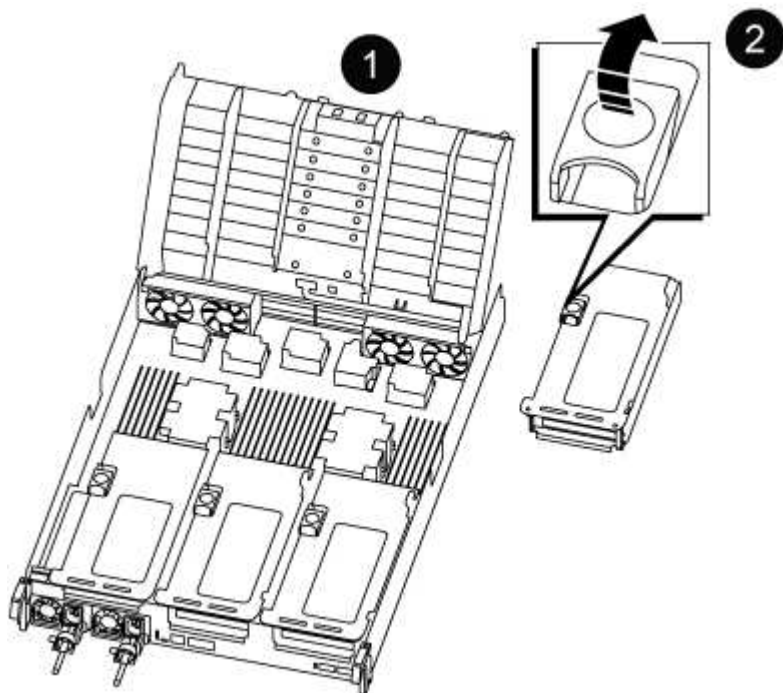
Step 3: Replace the RTC battery

Original controller

1. Remove PCIe riser 2 (middle riser) from the 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 the fan modules.

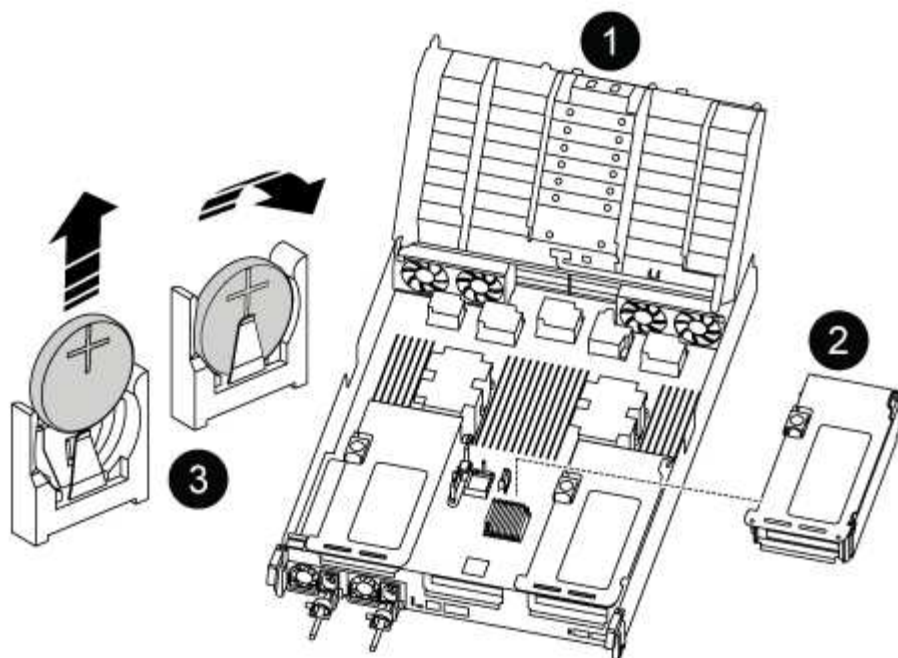
The riser raises up slightly from the controller module.

- c. Lift the riser up, shift it toward the fans so that the sheet metal lip on the riser clears the edge of the controller module, lift the riser out of the controller module, and then place it on a stable, flat surface.



1	Air duct
2	Riser 2 (middle riser) locking latch

2. Locate the RTC battery under Riser 2.



1	Air duct
2	Riser 2
3	RTC battery and 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.

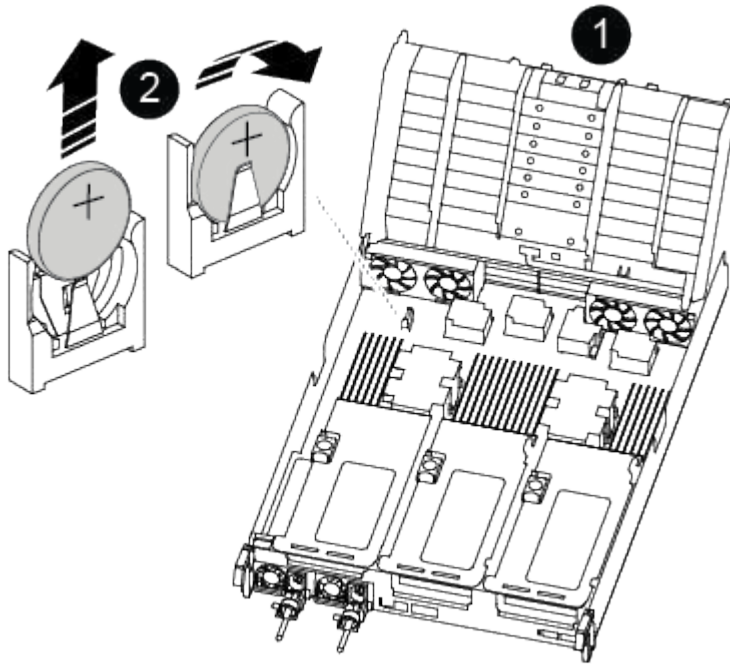
4. Remove the replacement battery from the antistatic shipping bag.
5. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
6. Visually inspect the battery to make sure that it is completely installed into the holder and that the polarity is correct.
7. Install the riser into the controller module:
 - a. Align the lip of the riser with the underside of the controller module sheet metal.
 - b. Guide the riser along the pins in the controller module, and then lower the riser into the controller module.
 - c. Swing the locking latch down and click it into the locked position.

When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

- d. Reinsert any SFP modules that were removed from the PCIe cards.

VER2 controller

1. Locate the RTC battery near the DIMMs.



1	Air duct
2	RTC battery and housing

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. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
5. 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

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. Complete the reinstallation of the controller module:

- a. 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.

- b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
- c. Plug the power cords into the power supplies, reinstall the power cable locking collar, and then connect the power supplies to the power source.

The controller module begins to boot as soon as power is restored. Be prepared to interrupt the boot process.

- d. If you have not already done so, reinstall the cable management device.
- e. Halt the controller at the LOADER prompt.

5. 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.

6. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.

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

8. 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 and Replacements](#) page for further information.

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

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

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

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