



ASA A800 systems

Install and maintain

NetApp
October 30, 2024

Table of Contents

- ASA A800 systems 1
 - Install and setup 1
 - Maintain 17

ASA A800 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 A800

This page gives graphic instructions for a typical installation of your system from racking and cabling, through initial system bring-up. Use the [AFF A800 Installation and Setup Instructions](#) if you are familiar with installing NetApp systems.



The ASA A800 uses the same installation procedure as the AFF A800 system.

Video steps - ASA A800

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

["Animation - Installation and Setup of an AFF A800"](#)



The ASA A800 uses the same installation procedure as the AFF A800 system.

Detailed steps - ASA A800

This page gives detailed step-by-step instructions for installing an ASA A800 system.

Step 1: Prepare for installation

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

You need to have access to the [NetApp Hardware Universe](#) (HWU) for information about site requirements as

well as additional information on your configured system. You might also want to have access to the [Release Notes for your version of ONTAP](#) for more information about this system.

What you need

You need to provide the following at your site:

- Rack space for the storage system
- Phillips #2 screwdriver
- Additional networking cables to connect your system to your network switch and laptop or console with a Web browser
 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		HA interconnect
	X66211A-05 (112-00595), 0.5m;		Cluster interconnect network
	X66211-1 (112-00573), 1m		
	X66211-2 (112-00574), 2m;		Storage, Data
	X66211-5 (112-00576), 5m		
10 GbE cable	X6566B-3-R6 (112-00300), 3m;		Data
	X6566B-5-R6 (112-00301), 5m		
25 GbE cable	X66240A-2 (112-00598), 2m;		Data
	X66240A-5 (112-00600), 5m		

Connector type	Part number and length	Type of cable...	For...
RJ-45 (order dependent)	Not applicable		Management
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

- 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

- Install the rail kits, as needed.

[Installing SuperRail into a four-post rack](#)

- 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.

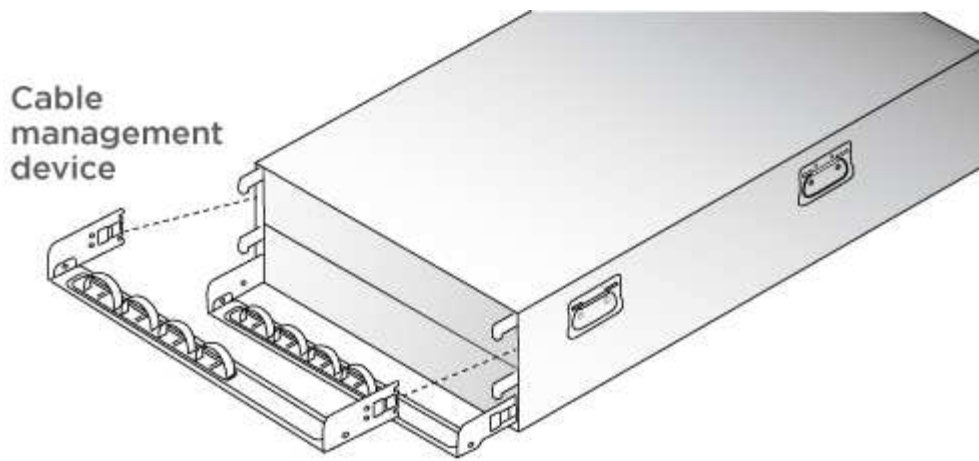
24 SSDs



48 SSDs



- 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.

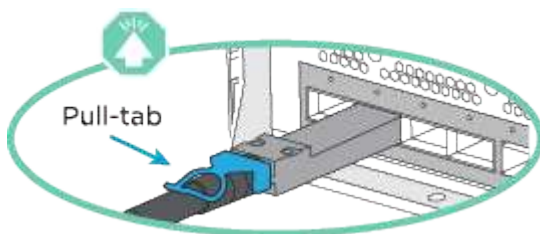
Option 1: Cable a two-node switchless cluster

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.




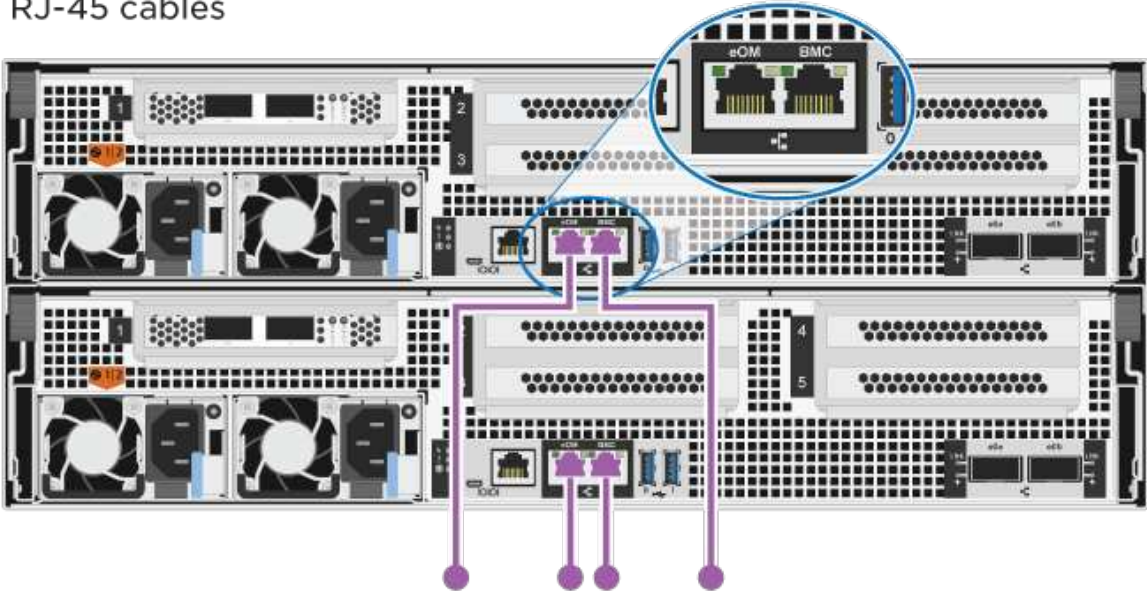

As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

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
<div data-bbox="181 163 256 212" data-label="Text">1</div>	<p data-bbox="318 163 716 191">Cable the HA interconnect ports:</p> <ul data-bbox="342 226 496 306" style="list-style-type: none"> • e0b to e0b • e1b to e1b <div data-bbox="380 331 1477 865" data-label="Image"> <p>The diagram illustrates the connection of High Availability (HA) interconnect ports on two controller modules. A blue 100 GbE cable is shown at the top left. Two circular callouts provide close-up views of the ports: the left callout shows a port labeled 'e0b' on a module, and the right callout shows a port labeled 'e1b' on a module. The main diagram shows two server racks. In the top rack, a blue cable connects the 'e0b' port of the left module to the 'e0b' port of the right module. In the bottom rack, a blue cable connects the 'e1b' port of the left module to the 'e1b' port of the right module. The racks contain various components including fans, network ports, and storage drives.</p> </div>
<div data-bbox="181 934 256 982" data-label="Text">2</div>	<p data-bbox="318 934 760 961">Cable the cluster interconnect ports:</p> <ul data-bbox="342 997 496 1077" style="list-style-type: none"> • e0a to e0a • e1a to e1a <div data-bbox="380 1102 1477 1656" data-label="Image"> <p>The diagram illustrates the connection of cluster interconnect ports on two controller modules. A green 100 GbE cable is shown at the top left. Two circular callouts provide close-up views of the ports: the left callout shows a port labeled 'e0a' on a module, and the right callout shows a port labeled 'e1a' on a module. The main diagram shows two server racks. In the top rack, a green cable connects the 'e0a' port of the left module to the 'e0a' port of the right module. In the bottom rack, a green cable connects the 'e1a' port of the left module to the 'e1a' port of the right module. The racks contain various components including fans, network ports, and storage drives.</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](#).

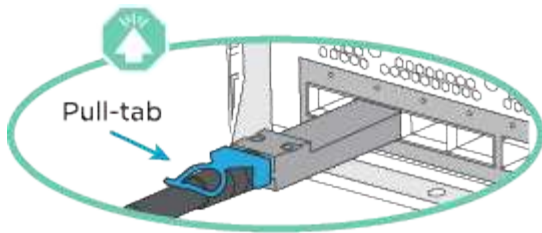
Option 2: Cable a switched cluster

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.



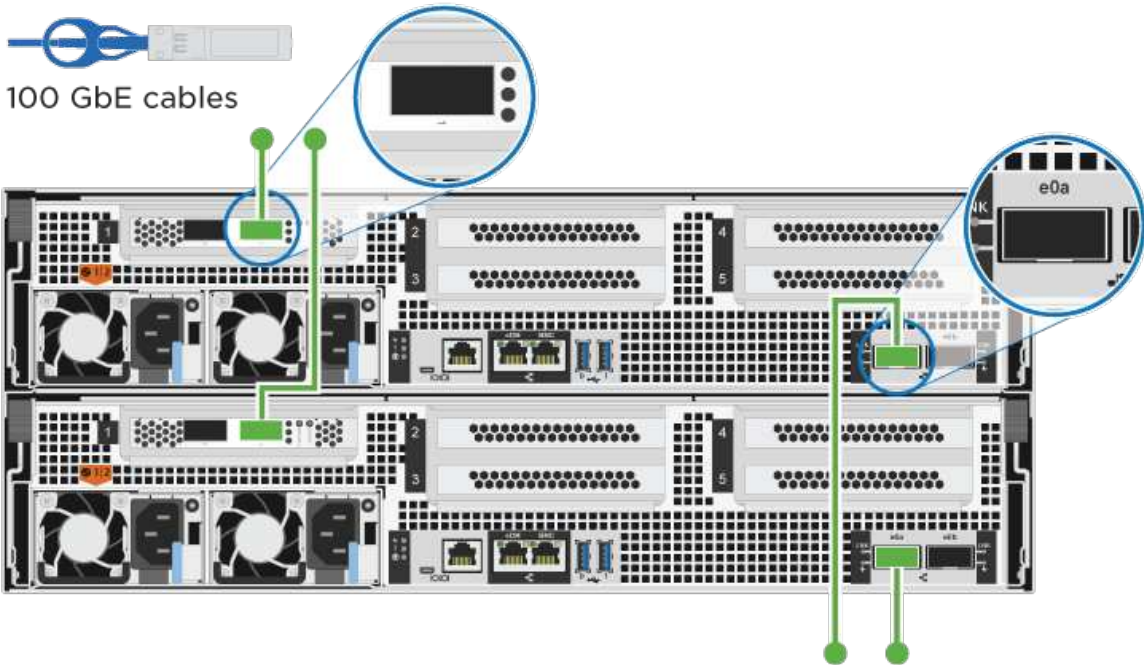
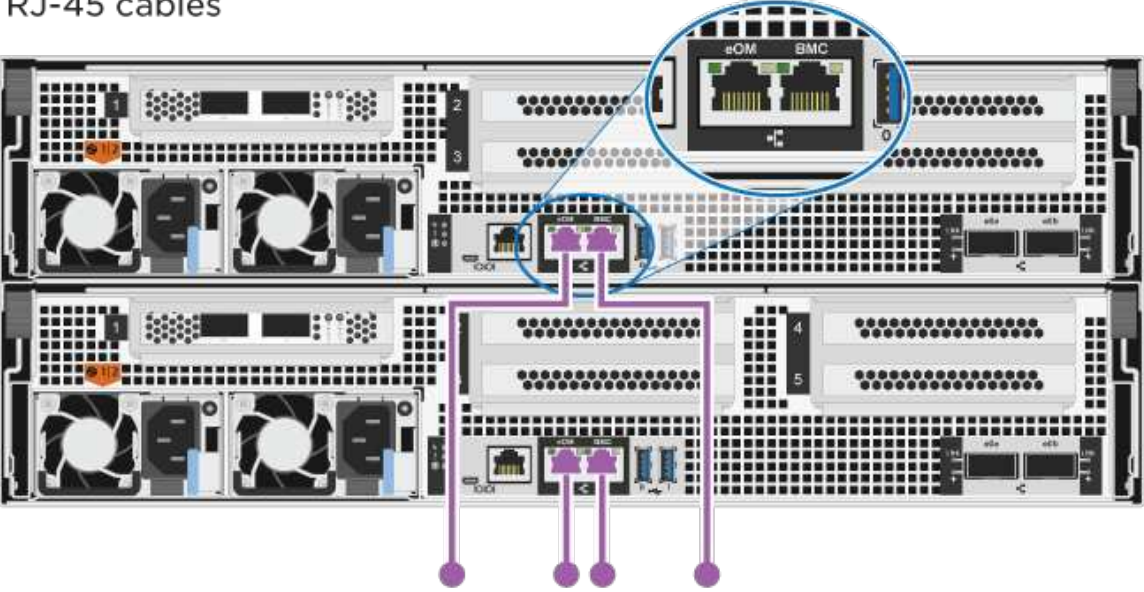
As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

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
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 to the 100 GbE cluster interconnect switches. e0a e1a</p>  <p>100 GbE cables</p>
3	<p>Cable the management ports to the management network switches</p>  <p>RJ-45 cables</p>
!	<p>DO NOT plug in the power cords at this point.</p>

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.

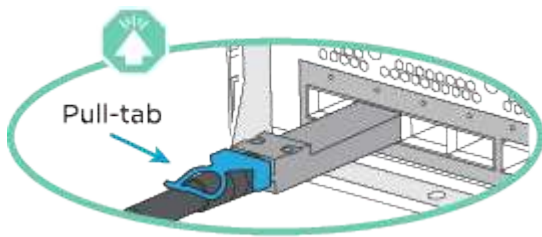
Option 1: Cable to a Fibre Channel host network

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

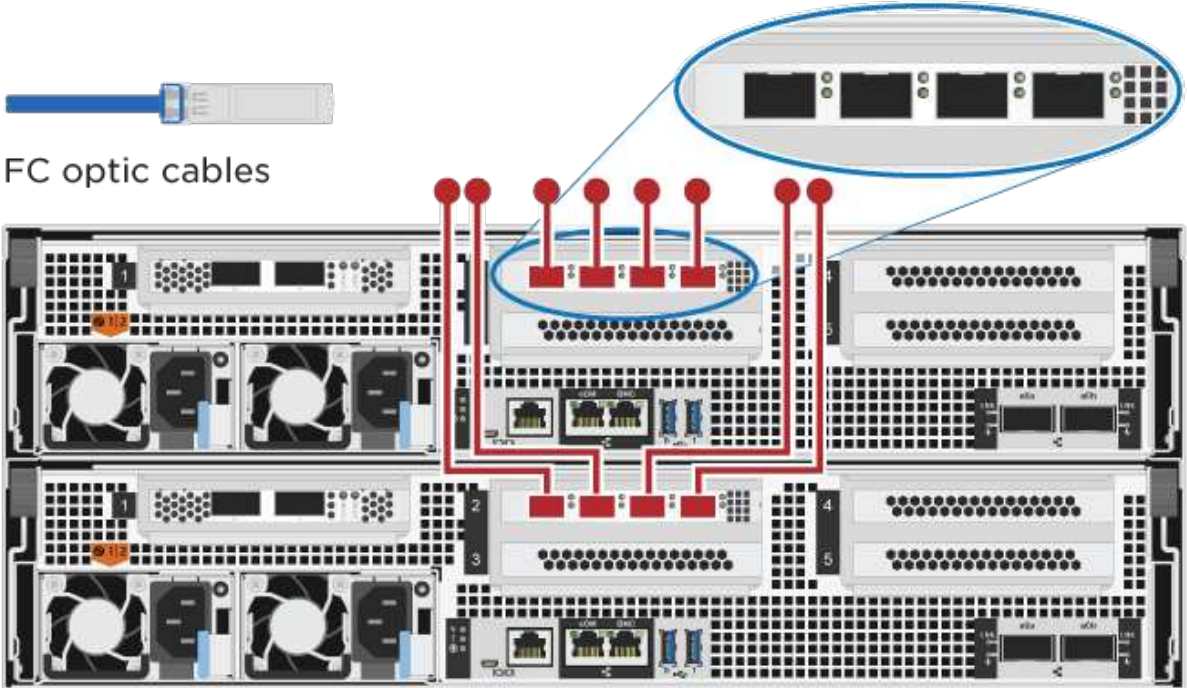
Before you begin

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>  <p>FC optic 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>

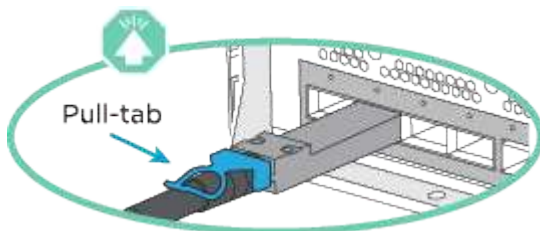
Option 2: Cable to a 10GbE host network

10GbE ports on the controllers are connected to 10GbE host network switches.

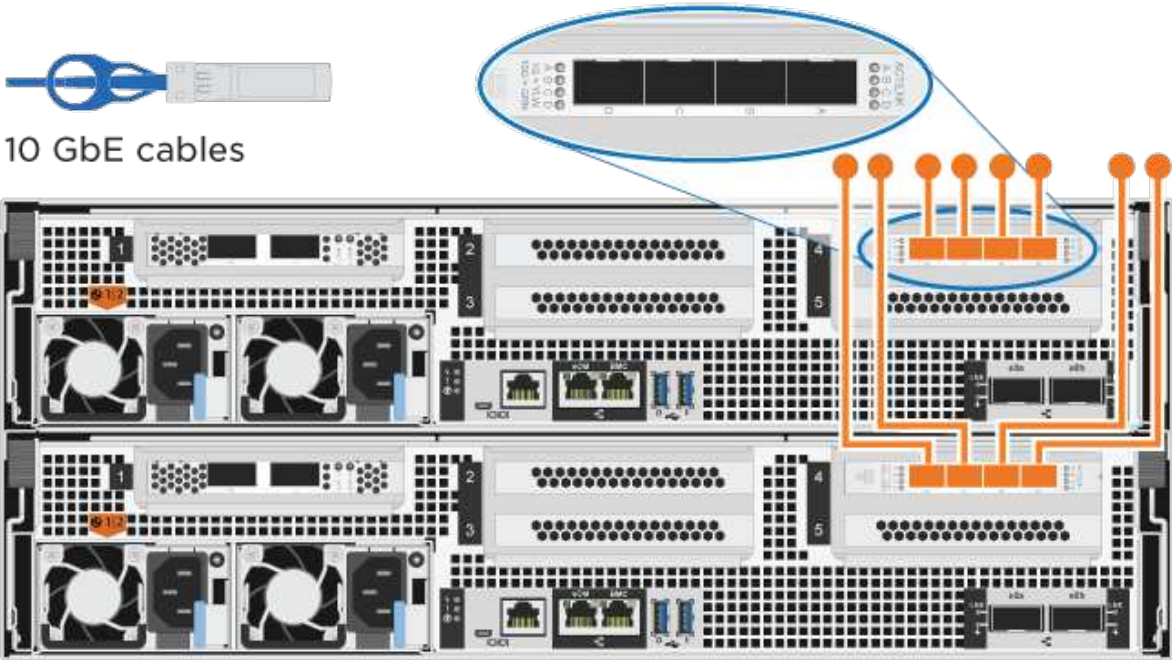
Before you begin

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.

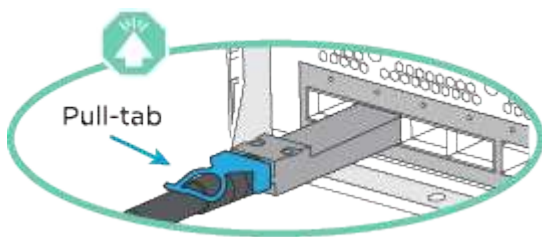
Step	Perform on each controller module
1	<p>Cable ports e4a through e4d to the 10GbE host network switches.</p>  <p>10 GbE cables</p>
2	<p>To perform other optional cabling, choose from:</p> <ul style="list-style-type: none"> • Option 3: Cable the controllers to a single drive shelf • Option 4: Cable 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

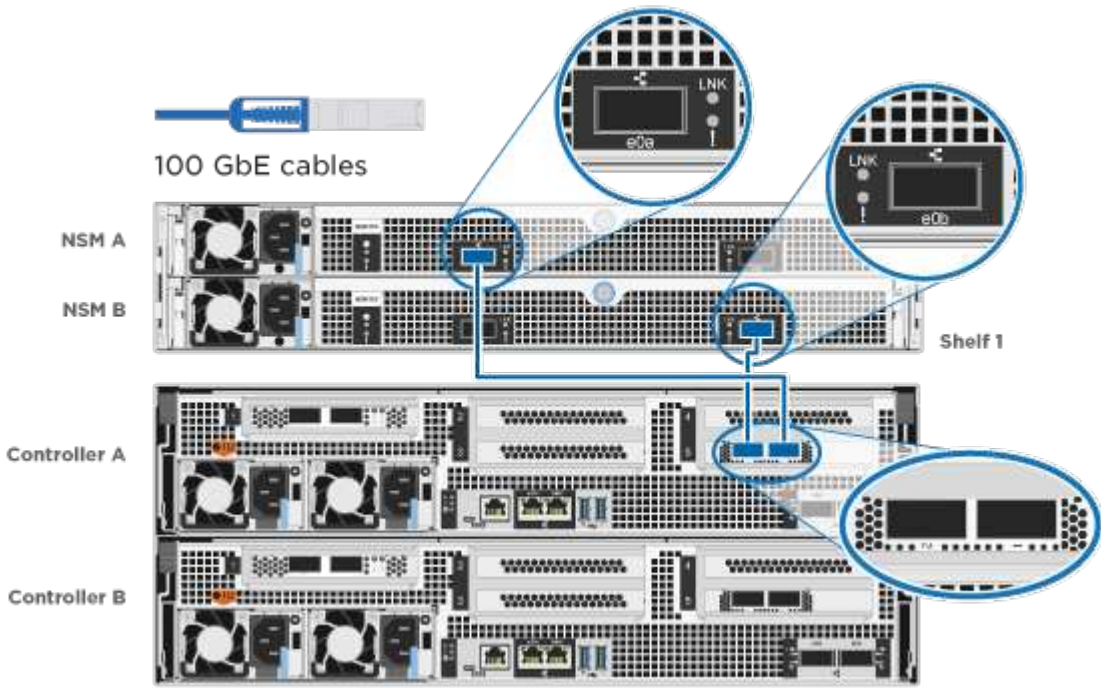
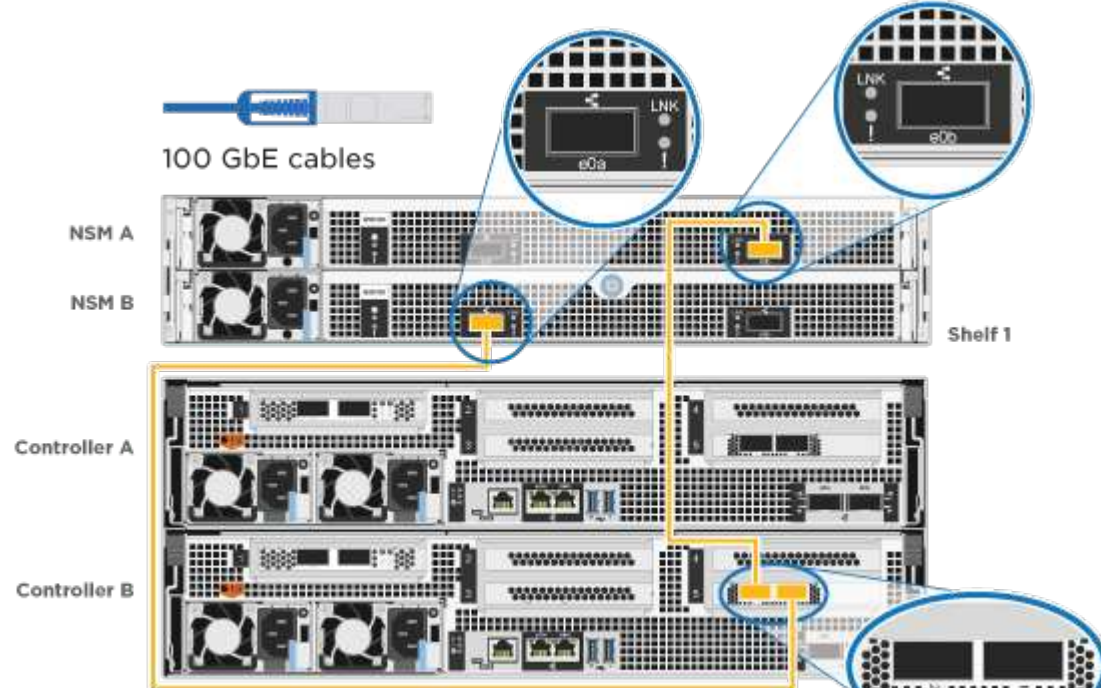
Be sure to check the illustration arrow for the proper cable connector pull-tab orientation.



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> 
2	<p>Cable controller B to the shelf:</p> 

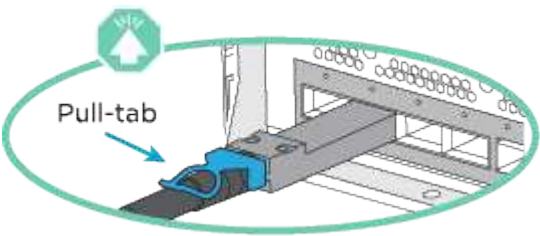
To complete setting up your system, see [Step 4: Complete system setup and configuration](#).

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.

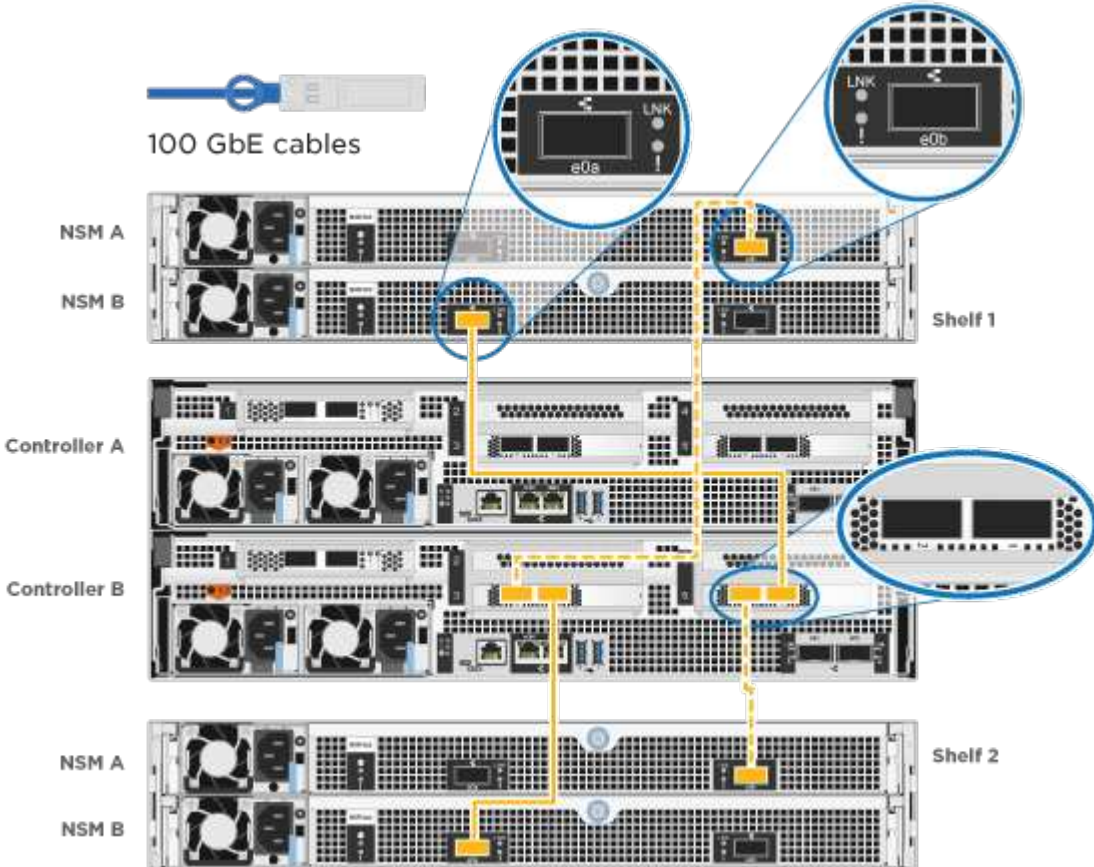


As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn it around and try again.

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
1	<p>Cable controller A to the shelves:</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 Service Modules (NSMs) on Shelf 1 and Shelf 2. Shelf 1 contains NSM A, NSM B, and Controller A. Shelf 2 contains NSM A and NSM B. 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 LNK and S0b ports on the NSM modules and the S0b port 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:

4. Select an ONTAP icon listed to discover:



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

 XXXXX is the system serial number for the target node.


System Manager opens.

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

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

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

Steps

1. Cable and configure your laptop or console:
 - a. Set the console port on the laptop or console to 115,200 baud with N-8-1.
-  See your laptop or console's online help for how to configure the console port.
- b. Connect the 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 the [ONTAP & ONTAP System Manager Documentation Resources](#) page for information about configuring additional features in ONTAP.

Maintain

Maintain ASA A800 hardware

For the ASA A800 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.

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

A PCIe (peripheral component interconnect express) card is an expansion card that plugs into the PCIe slot on 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

Overview of boot media replacement - ASA A800

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

Check encryption key support and status - ASA A800

Before shutting down the impaired controller, check if your version of ONTAP supports NetApp Volume Encryption (NVE) and if your key management system is properly configured.

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.

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.

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

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

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

- 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 you're 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 - ASA A800

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

Option 1: Most 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 - ASA A800

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

Step 1: Remove the controller module

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

5. Remove the cable management device from the controller module and set it aside.
6. 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

7. 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.

8. 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.



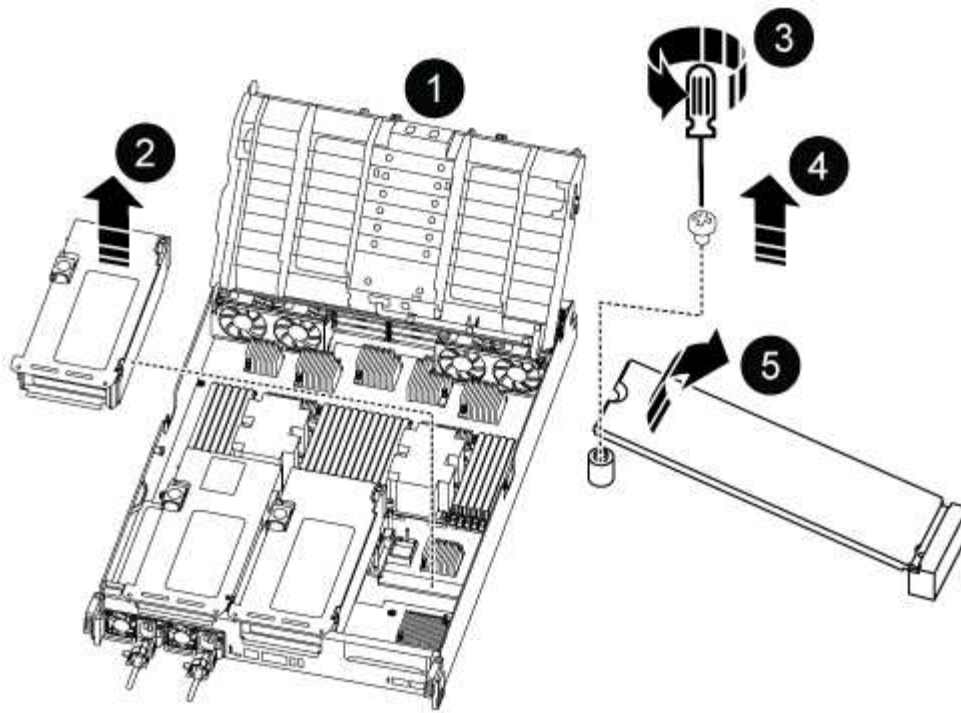
1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

Step 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:

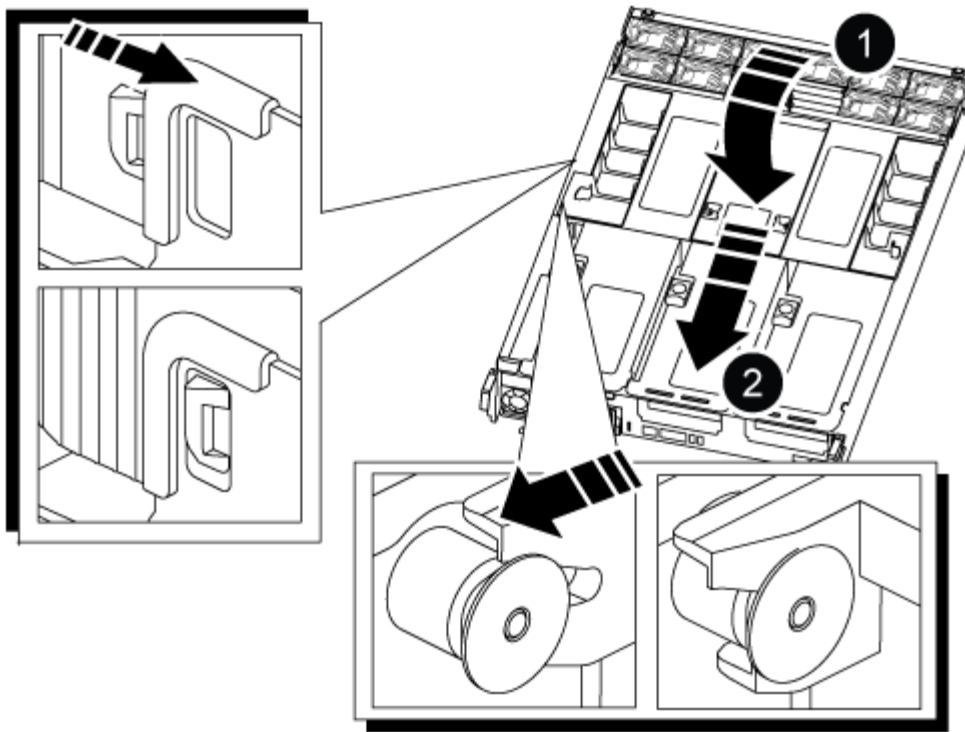
- boot
 - efi
- c. Copy the efi folder to the top directory on the USB flash drive.



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

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

- Plug the power cable into the power supply and reinstall the power cable retainer.
- 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.

- 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.

The controller begins to boot as soon as it is completely installed into the chassis.

- 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.

Boot the recovery image - ASA A800

Unresolved directive in asa800/bootmedia-recovery-image-boot-non-2n-mcc.adoc - include::.../_include/800_bootmedia_encryption_preshutdown_checks.adoc[]

Restore OKM, NSE, and NVE - ASA A800

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="621 153 829 191">Select option 10.</p> <p data-bbox="621 222 948 254">Show example boot menu</p> <div data-bbox="654 296 1456 1079"> <p data-bbox="683 333 1294 365">Please choose one of the following:</p> <ul data-bbox="683 411 1369 968" 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 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:

[illegible]

- 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-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTA1VT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUwQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxcilJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJsl+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----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-----
MIIEizCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
7yaumMQETNrpMfP+nQMd34y4AmseWYGM6qG0z37BRnYU0Wf2qDL61cQ3/jkm7Y94
EQBKG1NY8dVyjphmYZv+
-----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....
[Aug 29 21:06:28]: 0x808806100: 0: DEBUG: kmip2::main:
[initOpenssl]:460: 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, by entering the following command.

```
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 A800

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 A800

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 A800

Shut down the controllers so you can perform maintenance on the chassis.

This procedure is for systems with two node configurations. If you have a system with more than two nodes, see [How to perform a graceful shutdown and power up of one HA pair in a four node cluster](#).

Before you begin

- Stop all clients/host from accessing data on the NetApp system.
- Suspend external backup jobs.
- Make sure you have the necessary permissions and credentials:
 - Local administrator credentials for ONTAP.
 - NetApp onboard key management (OKM) cluster-wide passphrase if using storage encryption or NVE/NAE.
 - 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. Turn off AutoSupport and indicate how long you expect the system to be offline:

```
system node autosupport invoke -node * -type all -message "MAINT=8h Power Maintenance"
```

3. Identify the SP/BMC address of all nodes:

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

4. Exit the cluster shell: `exit`
5. Log into SP/BMC over SSH using the IP address of any of the nodes listed in the output from the previous step.

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



Open an SSH session to every SP/BMC connection so that you can monitor progress.

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

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

7. Enter **y** for each controller in the cluster when you see *Warning: Are you sure you want to halt node "cluster <node-name> number"? {y|n}:*

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

What's next?

- If the system is a NetApp StorageGRID or ONTAP S3 used as FabricPool cloud tier, refer to the [Gracefully shutdown and power up your storage system Resolution Guide](#) after performing this shutdown procedure.
- If using SSDs, refer to [SU490: \(Impact: Critical\) SSD Best Practices: Avoid risk of drive failure and data loss if powered off for more than two months](#) after performing this shutdown procedure.

Replace chassis - ASA A800

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

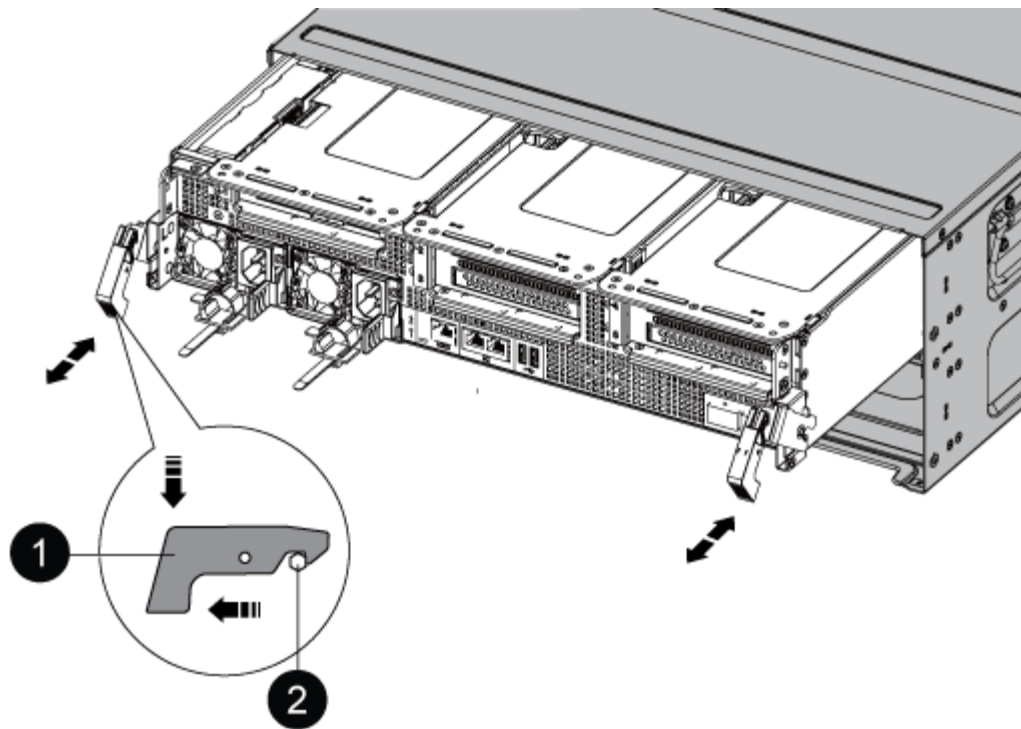
To replace the chassis, you must remove the controller modules from the old chassis.

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. Plug the power cables into the power supplies and reinstall the power cable retainers.
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.

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

- b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
 - c. If you have not already done so, reinstall the cable management device.
 - d. Interrupt the normal boot process by pressing `Ctrl-C`.
5. Repeat the preceding steps to install the second controller into the new chassis.

Complete chassis replacement - ASA A800

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 replacement - ASA A800

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 A800

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



When you see *Do you want to disable auto-giveback?*, enter *y*.

- 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	Take over or halt the impaired controller from the healthy controller: <code>storage failover takeover -ofnode impaired_node_name</code> When the impaired controller shows Waiting for giveback..., press Ctrl-C, and then respond <i>y</i> .

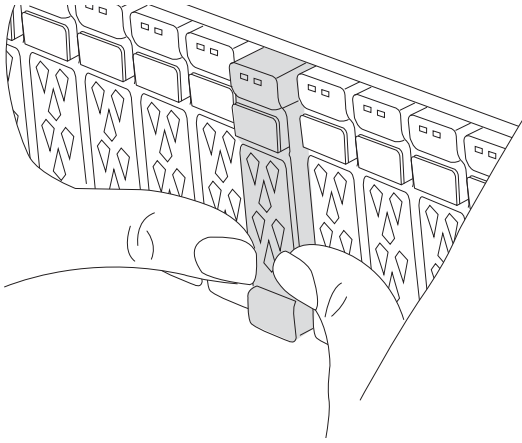
Replace the controller - ASA A800

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. On the front of the chassis, use your thumbs to firmly push each drive in until you feel a positive stop. This ensures that the drives are firmly seated against the chassis midplane.

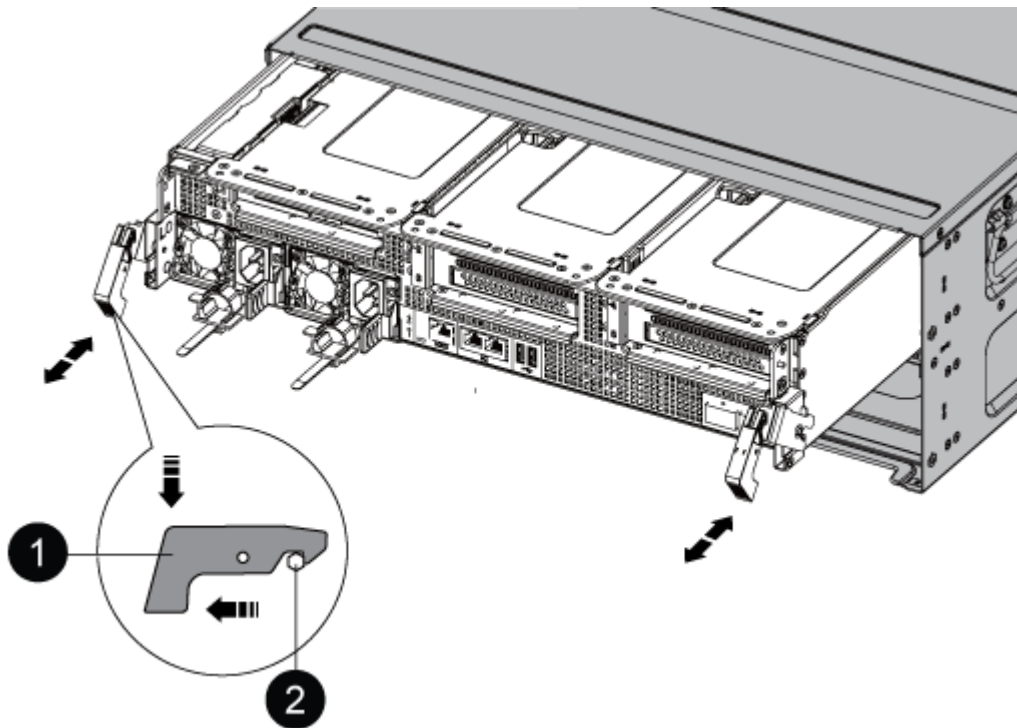


2. Go to the rear of the chassis. If you are not already grounded, properly ground yourself.
3. Unplug the controller module power supplies from the source.
4. Release the power cable retainers, and then unplug the cables from the power supplies.
5. Loosen the hook and loop strap binding the cables to 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

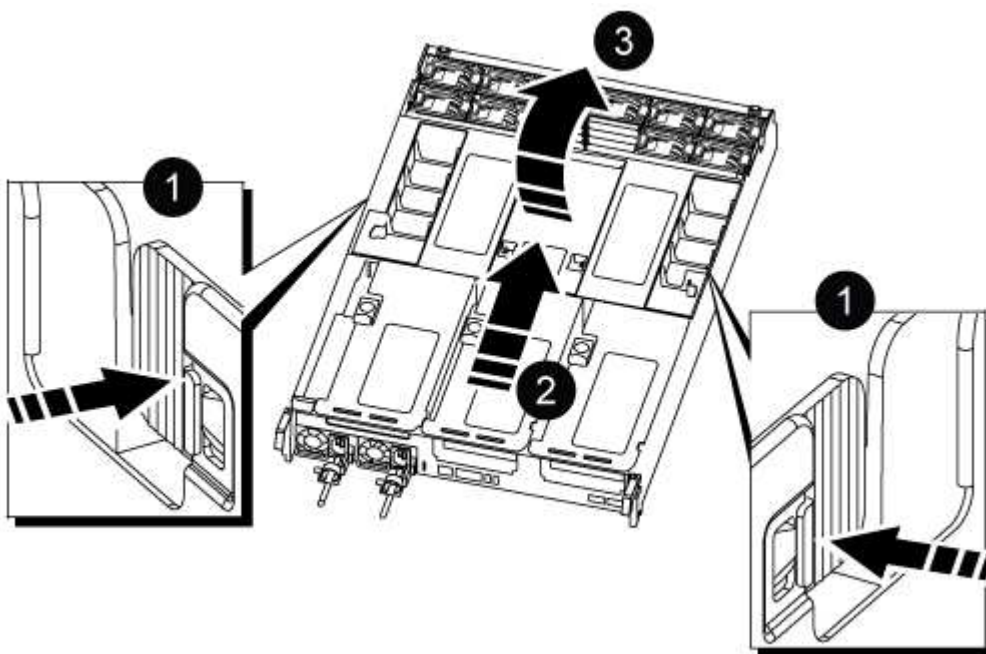
8. Slide the controller module out of the chassis and place it on a stable, flat surface.

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

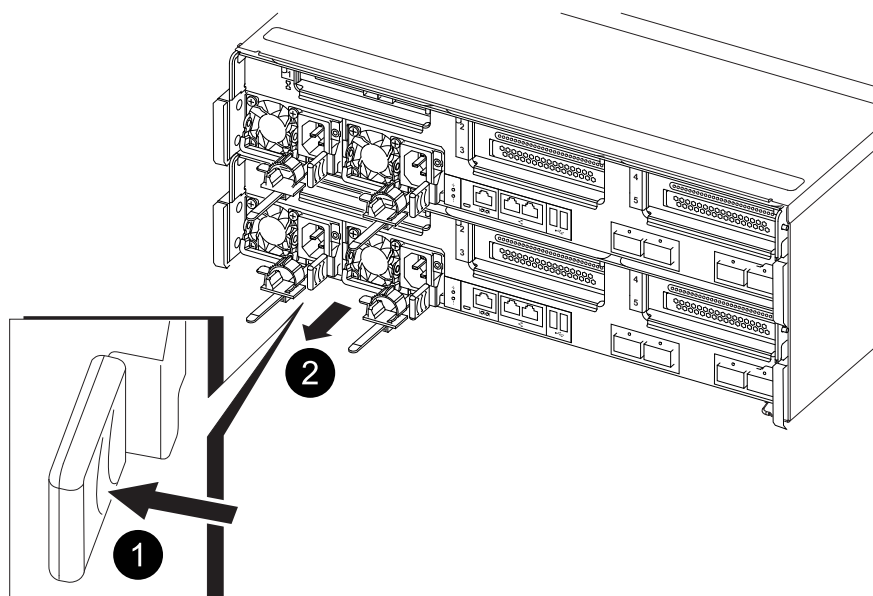
Step 2: Move the power supplies

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.

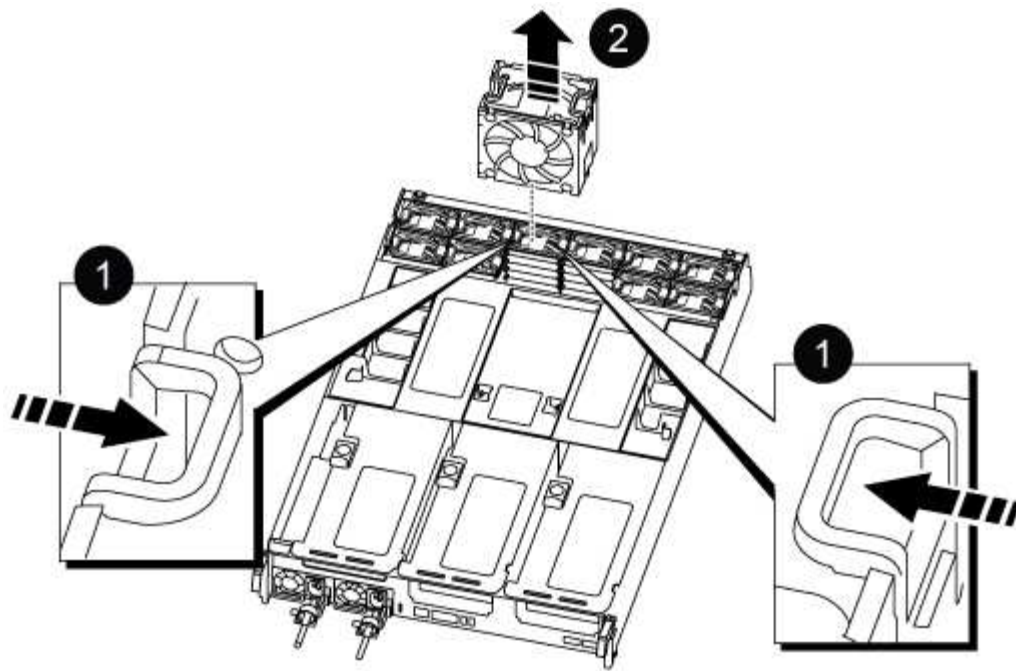


To avoid damaging the internal connector, do not use excessive force when sliding the power supply into the system.

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

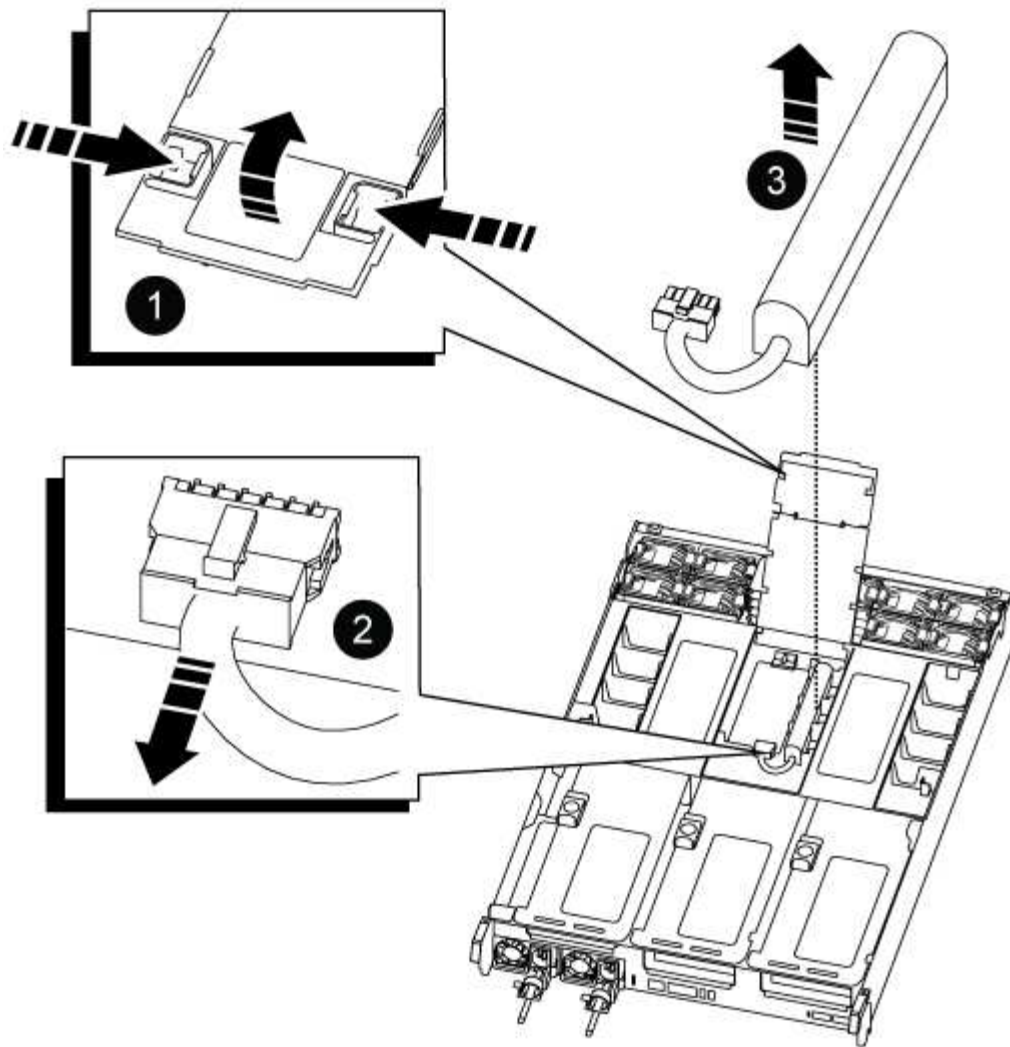
Fan module

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.

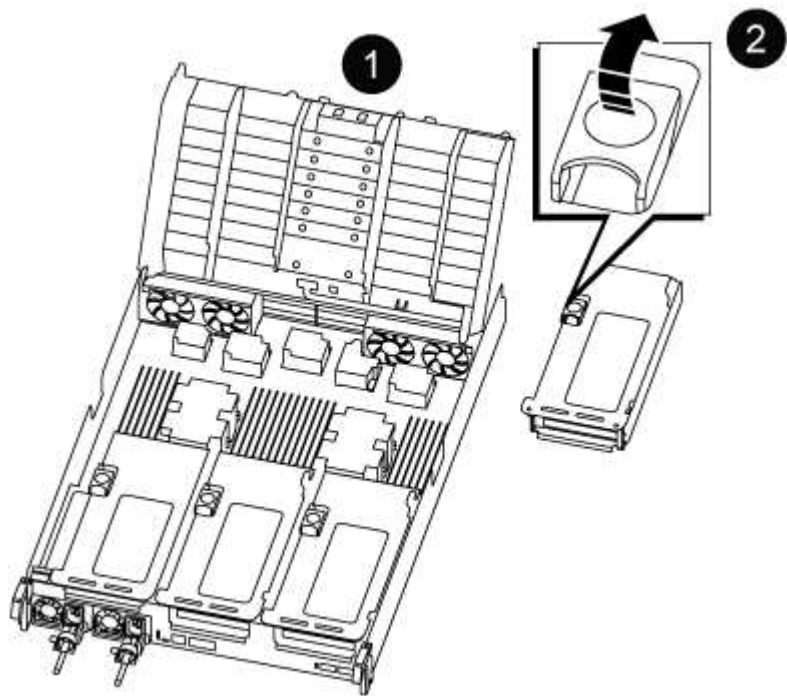
Step 5: Remove the PCIe risers

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.



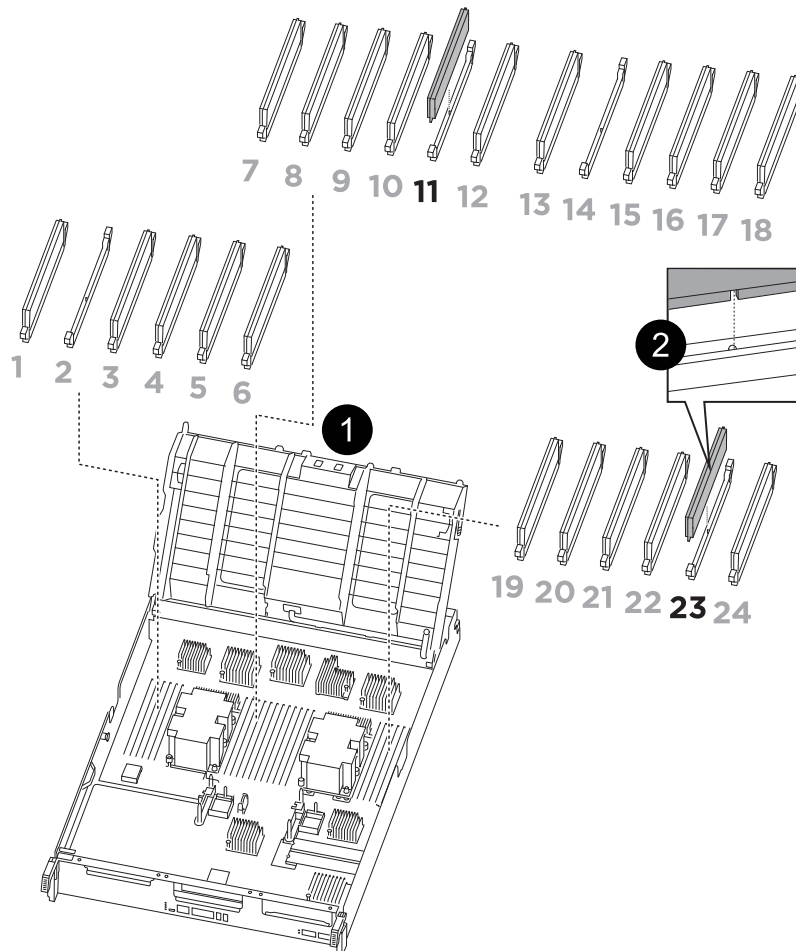
Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

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.

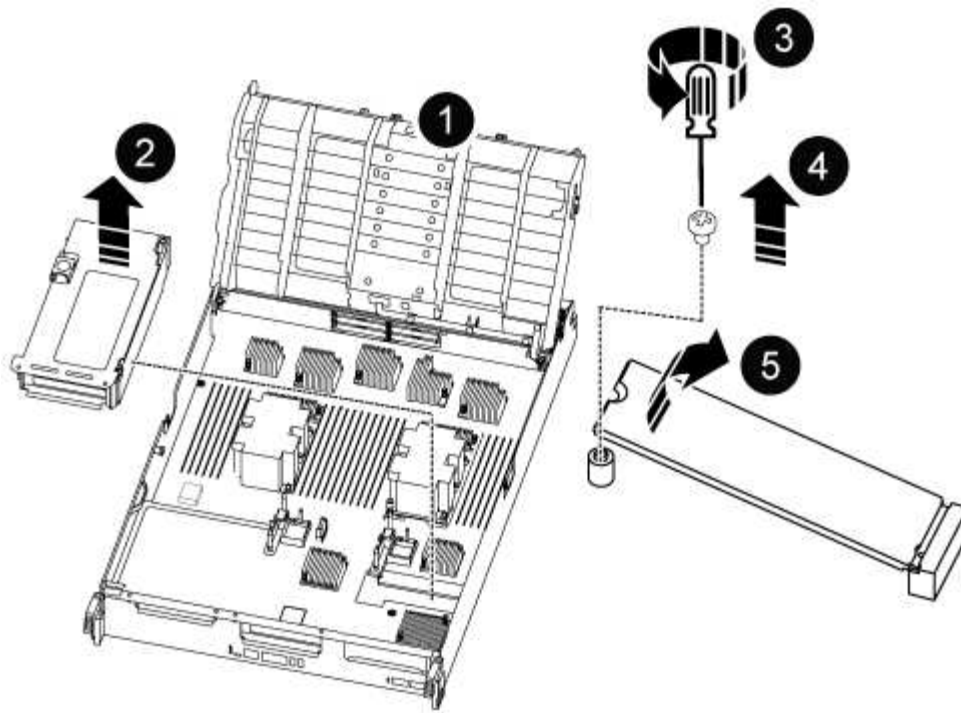
6. Push carefully, but firmly, on the top edge of the NVDIMM until the ejector tabs snap into place over the notches at the ends of the NVDIMM.
7. Repeat the preceding steps to move the other NVDIMM.

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.

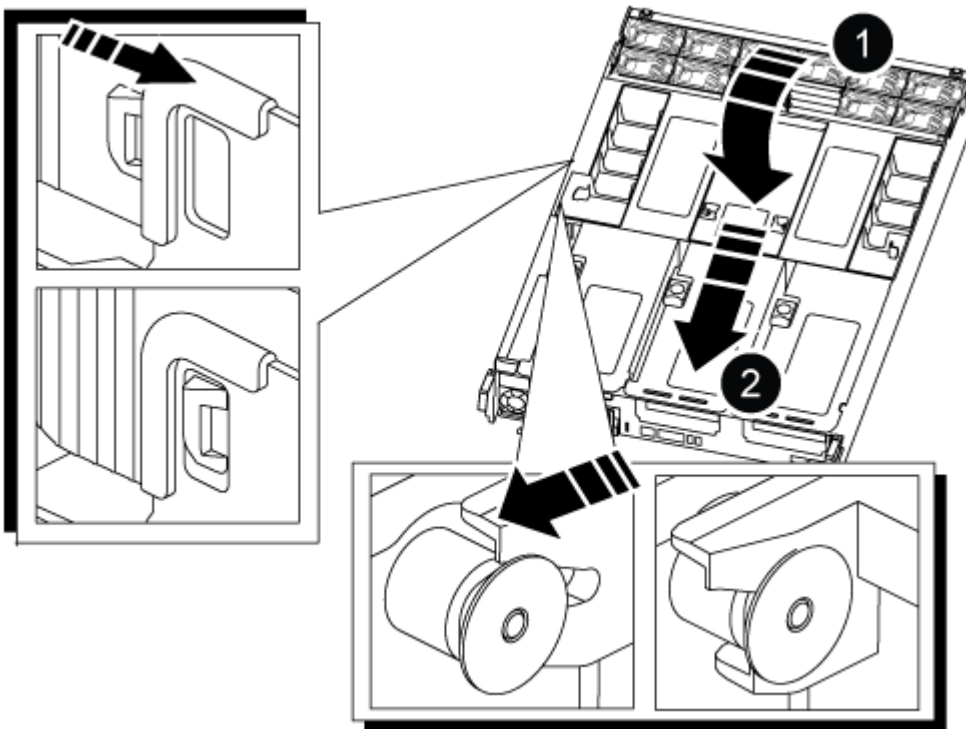
When locked, the locking latch is flush with the top of the riser and the riser sits squarely in the controller module.

- 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 A800

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 A800

Continue the replacement procedure by recabling the storage and confirming disk

reassignment.

Step 1: Recable the system

Recable the controller module’s storage and network connections.

Steps

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

Step 2: Reassign disks

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

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

- 1. If the *replacement* controller is in Maintenance mode (showing the *> prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
- 2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch:`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:			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.

[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 Reserver	Aggregate Pool	Home	Owner	DR Home	Home ID	Owner ID	DR Home ID
1.0.0	aggr0_1	node1	node1	-	1873775277	1873775277	-
1873775277	Pool0						
1.0.1	aggr0_1	node1	node1		1873775277	1873775277	-
1873775277	Pool0						
.							
.							
.							

- 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.

- 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](#)

- 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 A800

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. If an AutoSupport maintenance window was triggered, end it by using the `system node autosupport invoke -node * -type all -message MAINT=END` command.
4. 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 DIMM - ASA A800

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

Recable the controller module's storage and network connections.

Steps

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

Step 2: 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. 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. 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.

5. Remove the cable management device from the controller module and set it aside.
6. 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

7. 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.

8. 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.

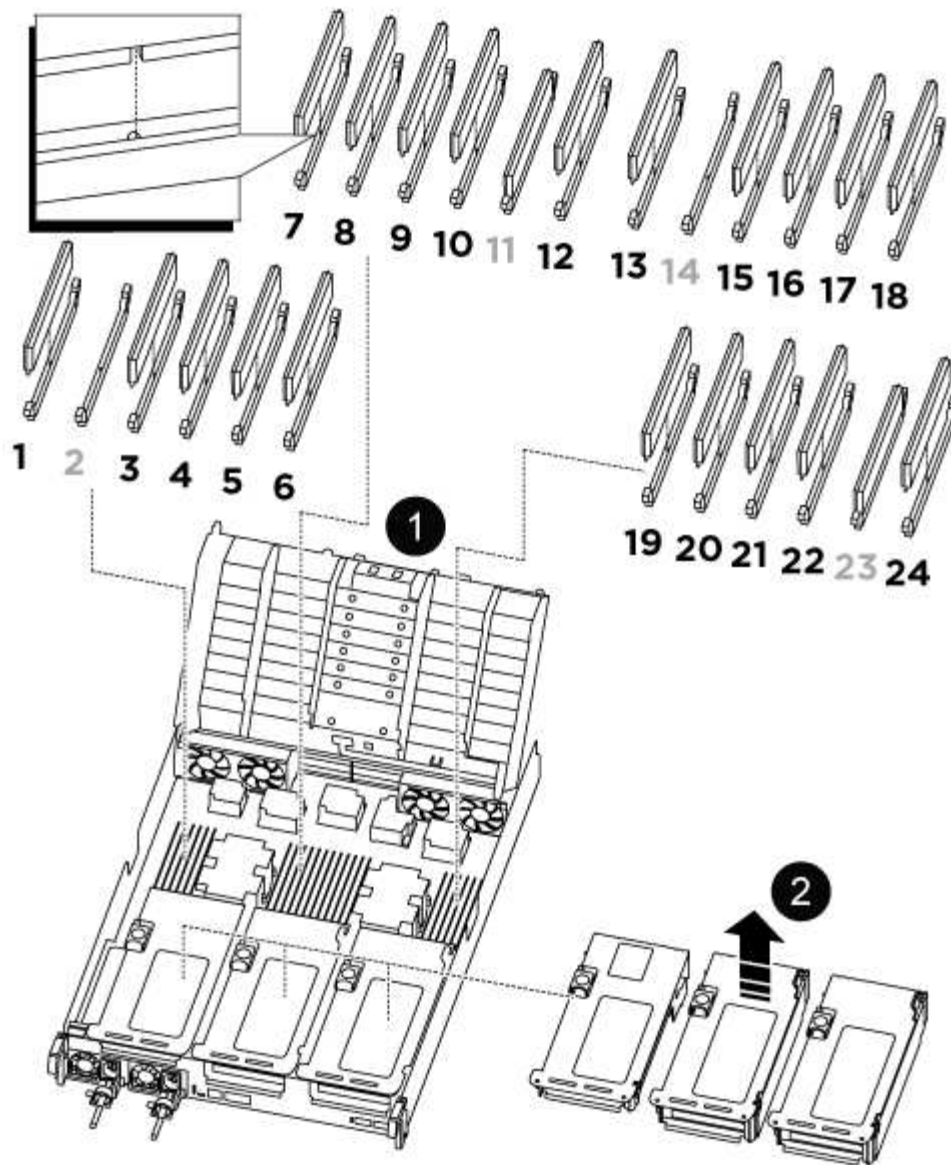


1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

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.



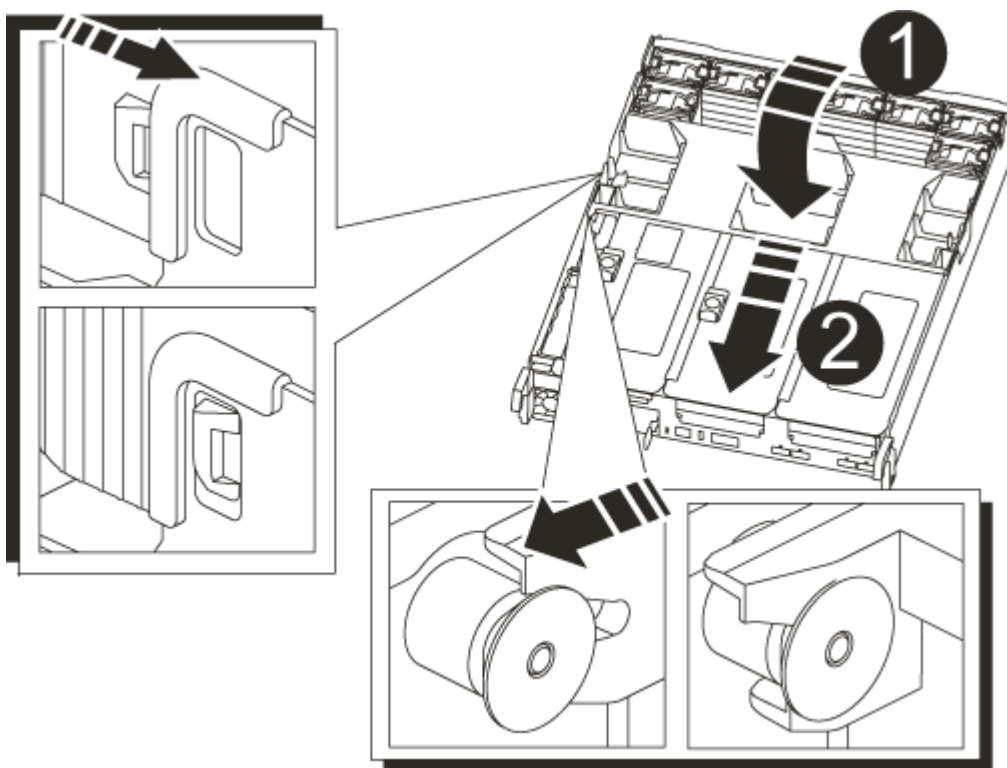
Visually inspect the DIMM to verify that it is evenly aligned and fully inserted into the slot.

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

- 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.

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

- Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.

- 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.

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

- Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
- 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 A800

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 replacement drive, if it is enabled



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

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

You can enter the command on either controller module.

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

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

You must disable automatic drive assignment on both controller modules.

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

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



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

4. Remove the failed drive:
 - a. Press the release button on the drive face to open the cam handle.
 - b. Slide the drive out of the shelf using the cam handle and supporting the drive with your other hand.

5. Wait a minimum of 70 seconds before inserting the replacement drive.

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

6. Insert the replacement drive:
 - a. With the cam handle in the open position, use both hands to insert the replacement drive.
 - b. Push until the drive stops.
 - c. Close the cam handle so that the drive is fully seated into the 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 reenables 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 reenables automatic drive assignment on both controller modules.

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

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

Option 2: Replace HDD

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



You manually assign drive ownership and then reenables 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 A800

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



When you see *Do you want to disable auto-giveback?*, enter `y`.

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</pre> <p>When the impaired controller shows Waiting for giveback..., press Ctrl-C, and then respond <i>y</i>.</p>

Step 2: Remove the controller module

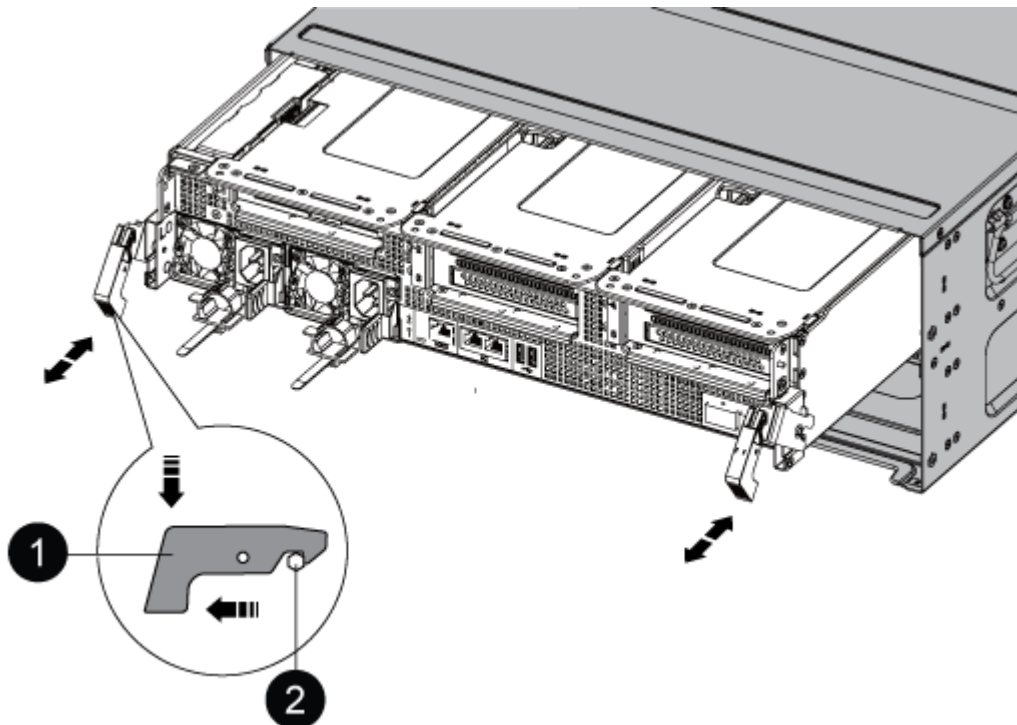
You must remove the controller module from the chassis when you replace a fan module.

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

5. Remove the cable management device from the controller module and set it aside.
6. 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

7. Slide the controller module out of the chassis.

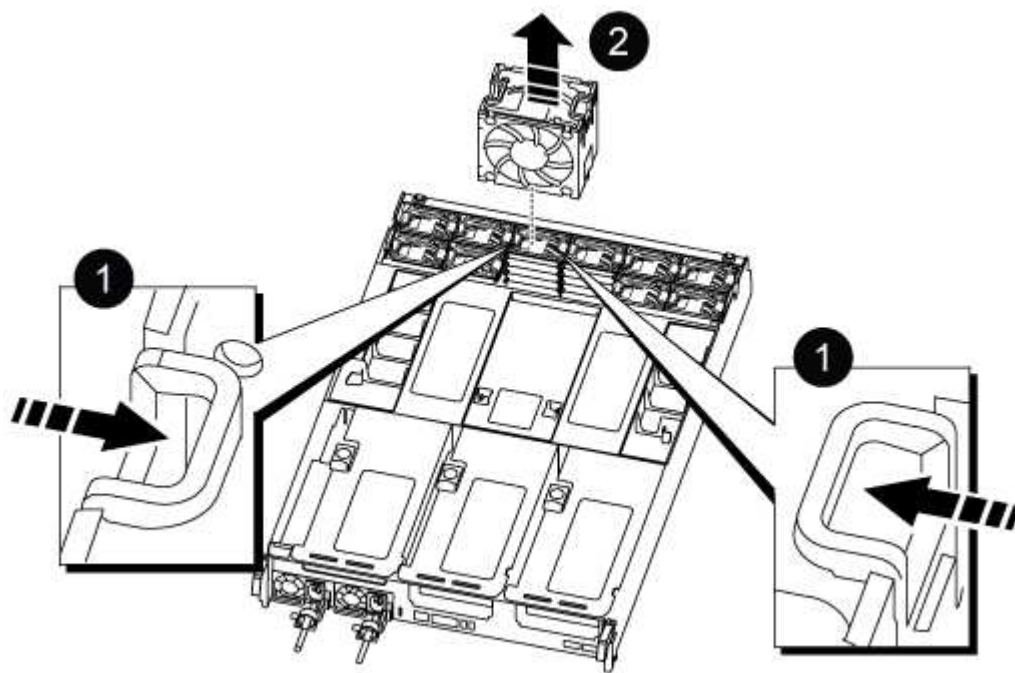
Make sure that you support the bottom of the controller module as you slide it out of the chassis.

8. 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

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 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.

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.
3. Plug the power cables into the power supplies and reinstall the power cable retainers.
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.

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

- b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
 - c. If you have not already done so, reinstall the cable management device.
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 -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 A800

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



When you see *Do you want to disable auto-giveback?*, enter *y*.

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	Take over or halt the impaired controller from the healthy controller: <code>storage failover takeover -ofnode impaired_node_name</code> When the impaired controller shows Waiting for giveback..., press Ctrl-C, and then respond <i>y</i> .

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.

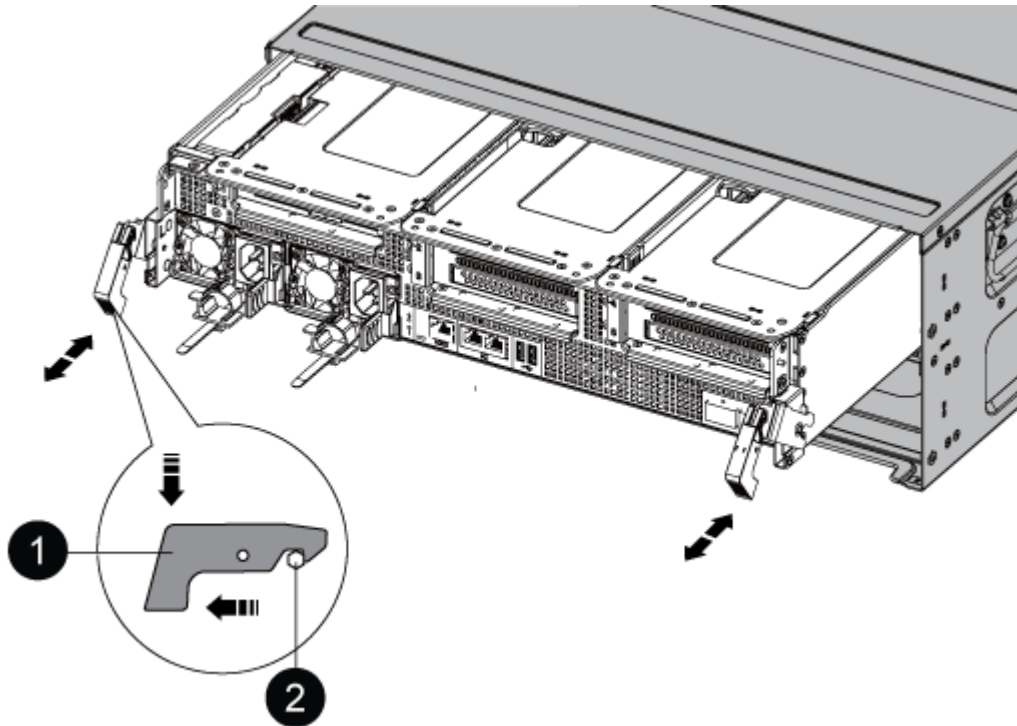
1. If you are not already grounded, properly ground yourself.
2. Unplug the controller module power supplies from the source.
3. Release the power cable retainers, and then unplug the cables from the power supplies.

4. 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.

5. Remove the cable management device from the controller module and set it aside.
6. 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

7. 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.

8. 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.

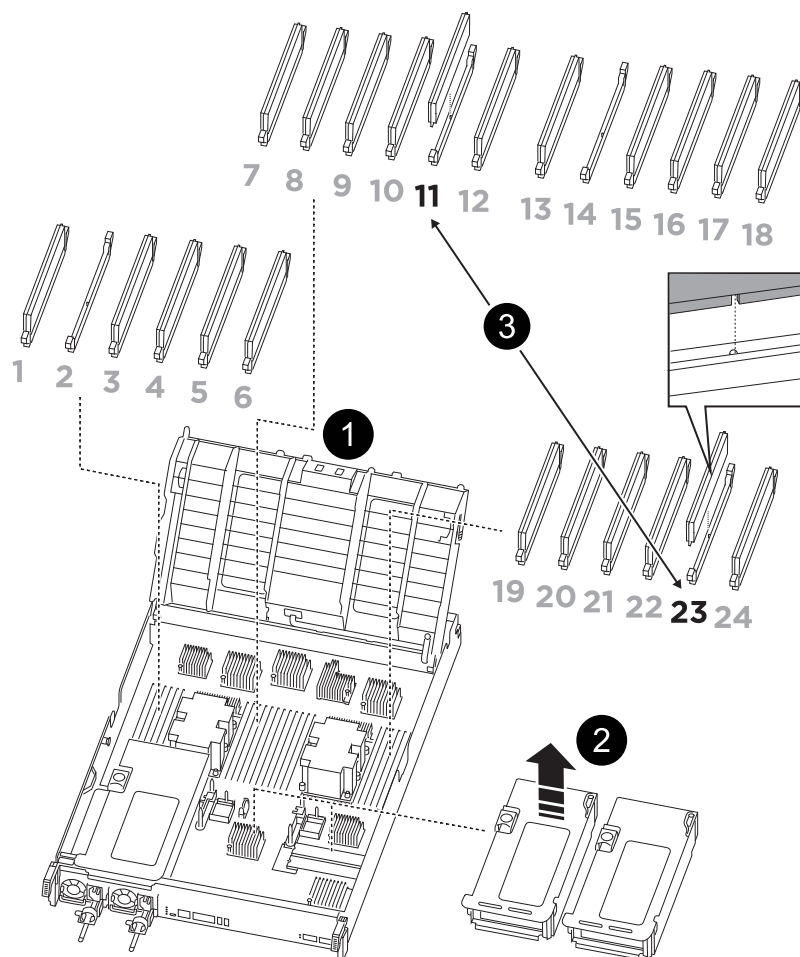


1	Air duct locking tabs
2	Slide air duct towards fan modules
3	Rotate air duct towards fan modules

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

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. 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.

5. 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.



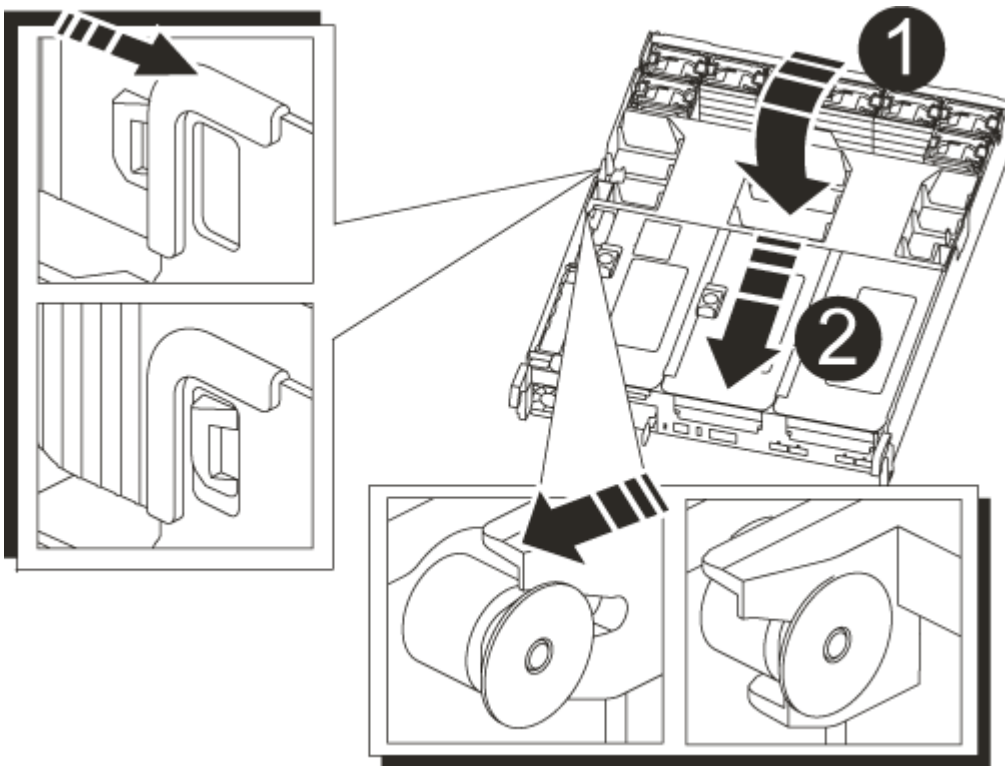
Visually inspect the NVDIMM to verify that it is evenly aligned and fully inserted into the slot.

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.



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. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
5. 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.

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

- b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
- c. 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 A800

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



When you see *Do you want to disable auto-giveback?*, enter *y*.

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: <pre>storage failover takeover -ofnode impaired_node_name</pre></p> <p>When the impaired controller shows Waiting for giveback..., press Ctrl-C, and then respond <i>y</i>.</p>

Step 2: Remove the controller module

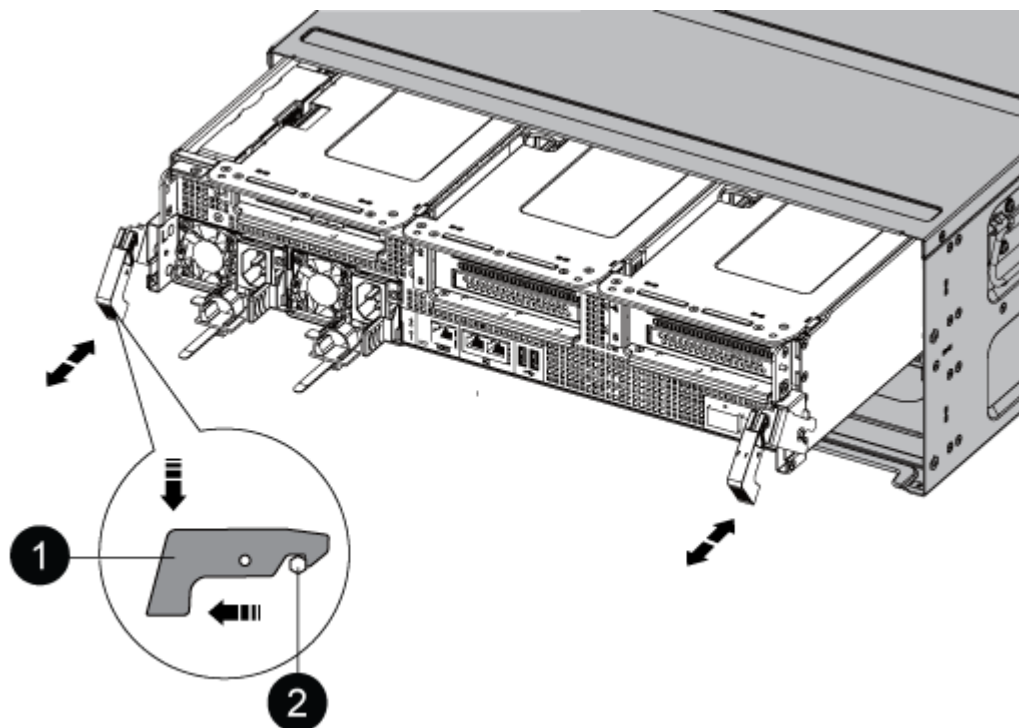
You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

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

5. Remove the cable management device from the controller module and set it aside.
6. 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

7. 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.

8. 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. Plug the power cord into the power supply, reinstall the power cable locking collar, and then connect the power supply to the power source.
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.

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

- b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
 - c. 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 PCIe card - ASA A800

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



When you see *Do you want to disable auto-giveback?*, enter *y*.

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: <code>storage failover takeover -ofnode <i>impaired_node_name</i></code></p> <p>When the impaired controller shows Waiting for giveback..., press Ctrl-C, and then respond <i>y</i>.</p>

Step 2: Remove the controller module

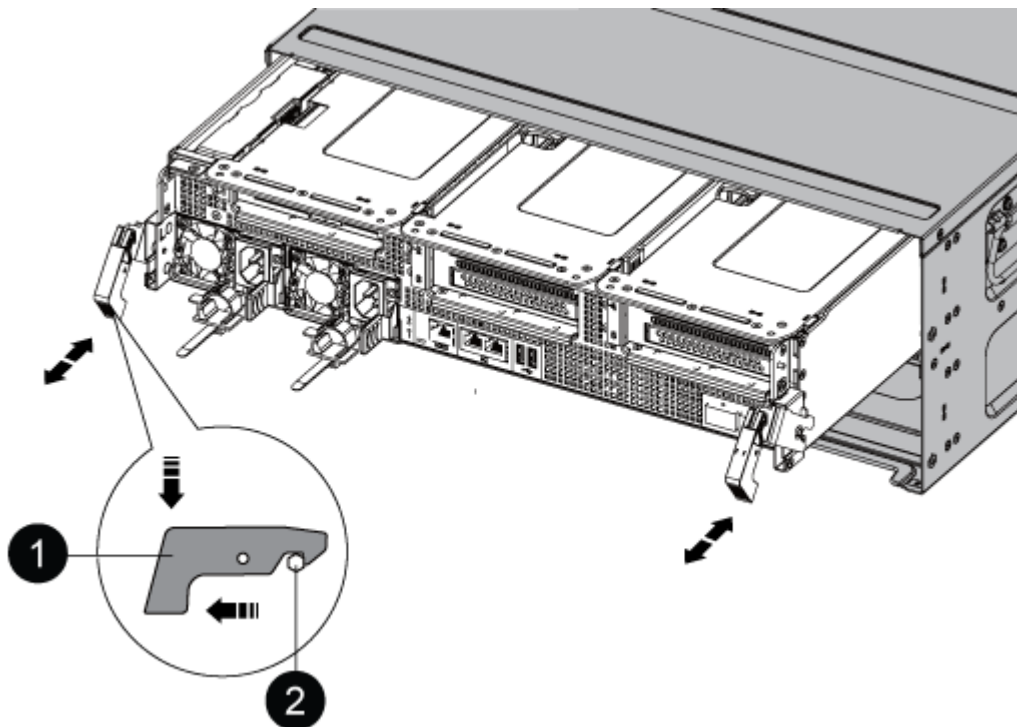
You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

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

5. Remove the cable management device from the controller module and set it aside.
6. 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.

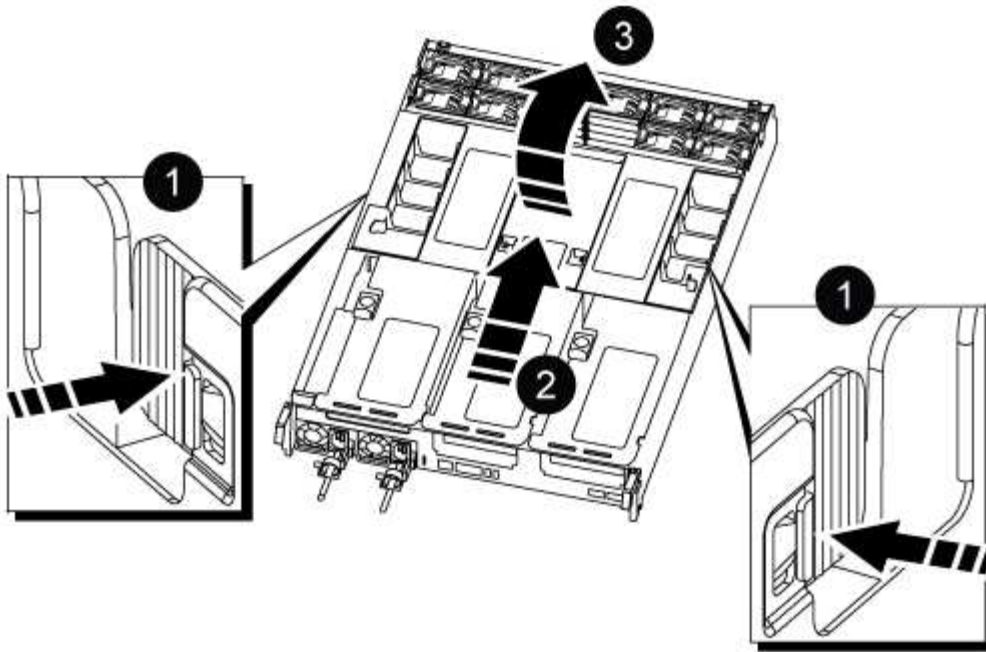


1	Locking latch
2	Locking pin

7. 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.

8. 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

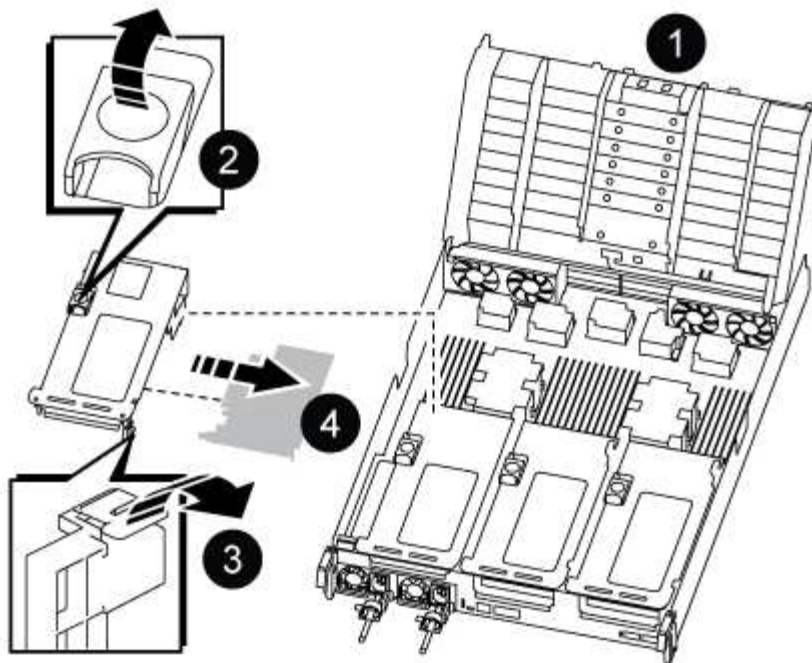
Step 3: Replace a PCIe card

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:

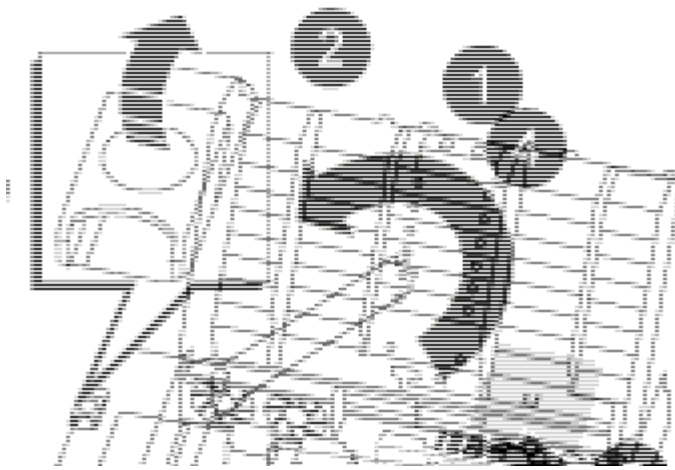
- a. Turn the riser so that you can access the PCIe card.
- b. Press the locking bracket on the side of the PCIe riser, and then rotate it to the open position.
- c. Remove the PCIe card from the riser.

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

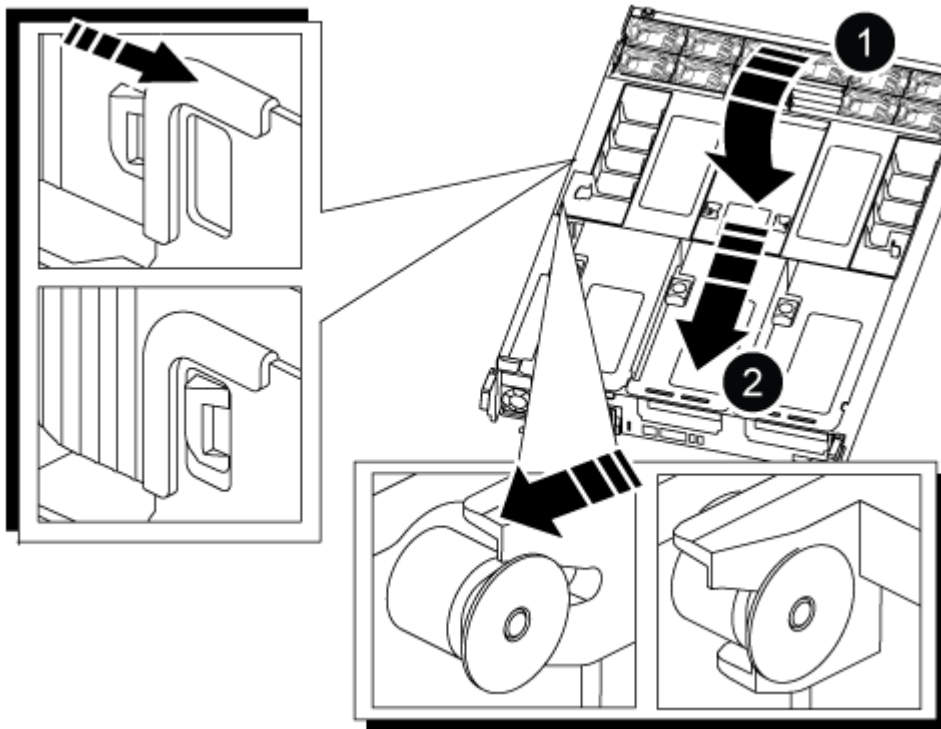
controller module.

- 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 power supply - ASA A800

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.

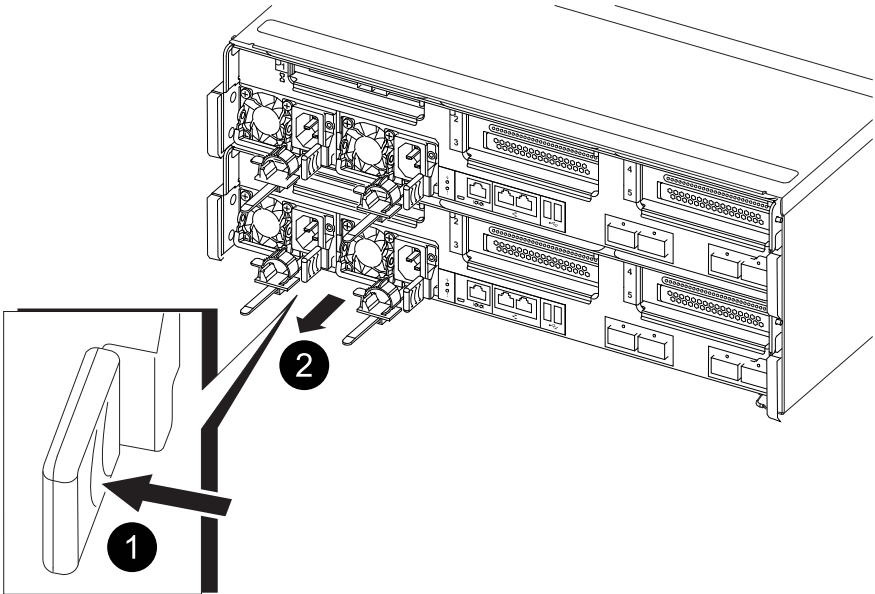
Option 1: Replace an AC PSU



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.



	Blue PSU locking tab
	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.

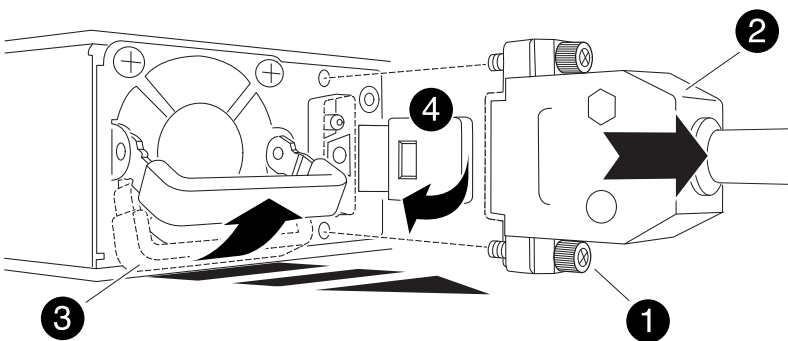
Option 2: Replace a DC PSU

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 A800

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



When you see *Do you want to disable auto-giveback?*, enter *y*.

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: <code>storage failover takeover -ofnode impaired_node_name</code></p> <p>When the impaired controller shows Waiting for giveback..., press Ctrl-C, and then respond <i>y</i>.</p>

Step 2: Remove the controller module

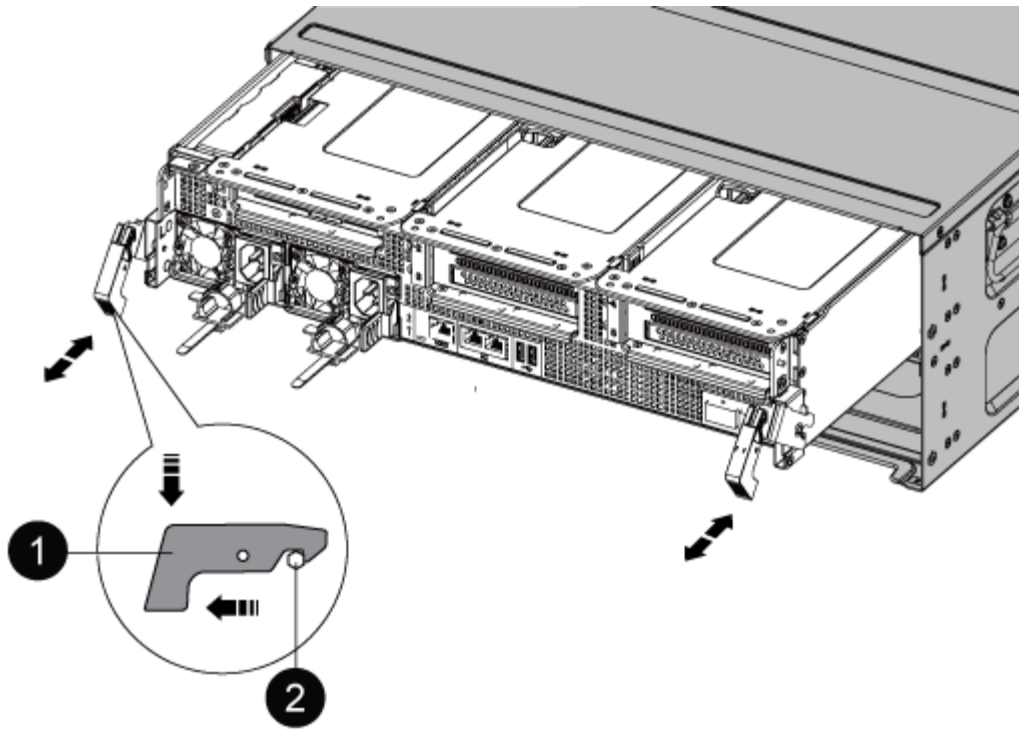
You must remove the controller module from the chassis when you replace the controller module or replace a component inside the controller module.

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

5. Remove the cable management device from the controller module and set it aside.
6. 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:

- 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

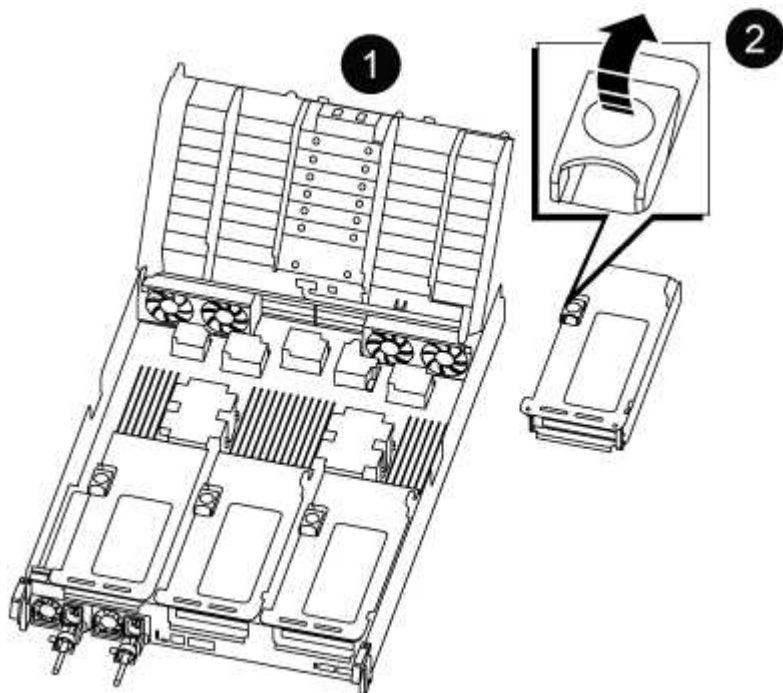
Step 3: Replace the RTC battery

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.

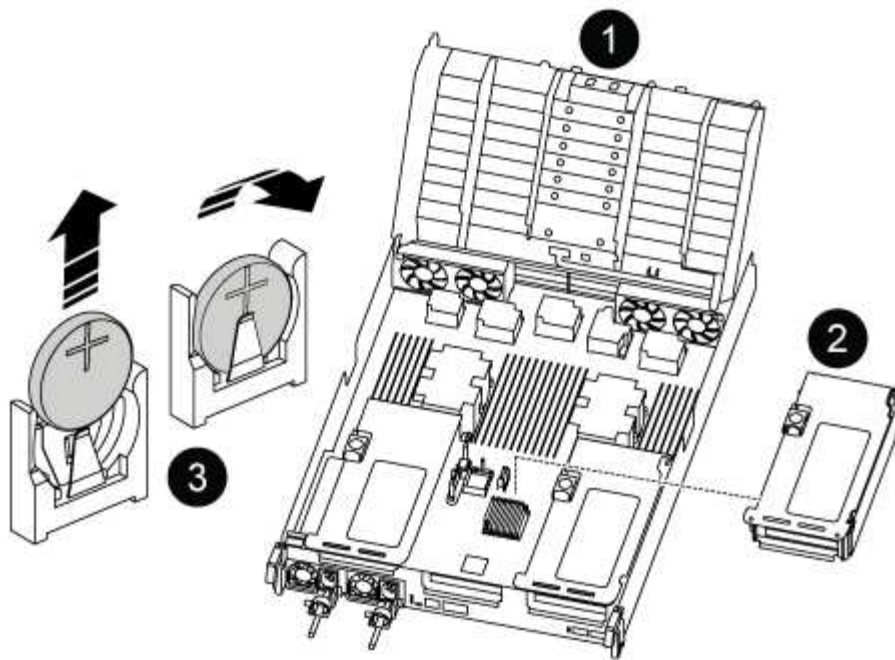
The riser raises up slightly from the controller module.

- 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.

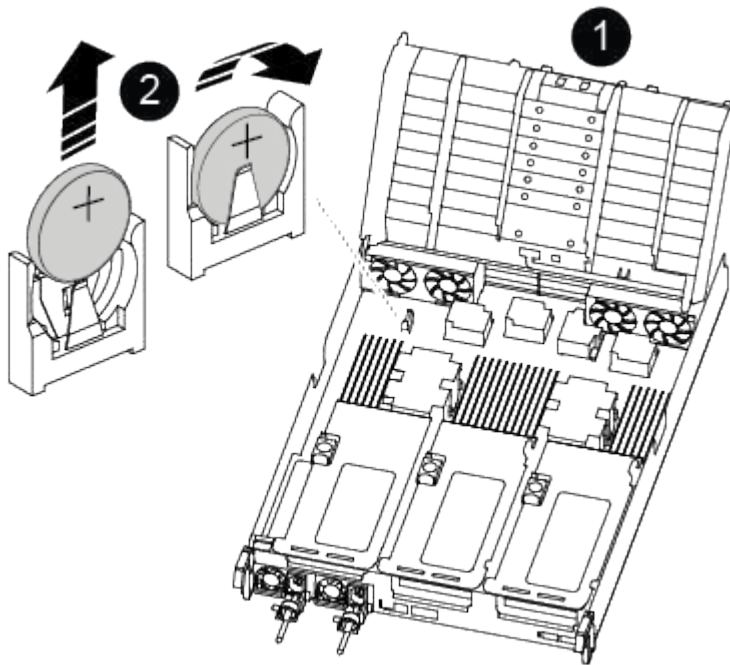
4. Remove the replacement battery from the antistatic shipping bag.
5. Note the polarity of the RTC battery, and then insert it into the holder by tilting the battery at an angle and pushing down.
6. Visually inspect the battery to make sure that it is completely installed into the holder and that the 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. If the power supplies were unplugged, plug them back in and reinstall the power cable retainers.
5. Complete the reinstallation of the controller module:

- a. 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.

- b. Rotate the locking latches upward, tilting them so that they clear the locking pins, and then lower them into the locked position.
 - c. If you have not already done so, reinstall the cable management device.
 - d. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
 - a. Check the date and time on the healthy controller with the `show date` command.
 - b. At the LOADER prompt on the target controller, check the time and date.
 - c. If necessary, modify the date with the `set date mm/dd/yyyy` command.
 - d. If necessary, set the time, in GMT, using the `set time hh:mm:ss` command.
 - e. Confirm the date and time on the target controller.
 7. At the LOADER prompt, enter `bye` to reinitialize the PCIe cards and other components and let the controller reboot.
 8. Return the controller to normal operation by giving back its storage: `storage failover giveback -ofnode impaired_node_name`
 9. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

Step 5: 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 © 2024 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.