



# **AFF A900 systems**

## **Install and maintain**

NetApp  
August 26, 2022

# Table of Contents

AFF A900 systems .....	1
Install and setup .....	1
Maintain .....	17

# AFF A900 systems

## Install and setup

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

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

- [Quick steps](#)

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

- [Video steps](#)

Video step-by-step instructions.

- [Detailed steps](#)

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

### Quick steps - AFF A900

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

Access the *Installation and Setup Instructions* PDF poster:

[AFF A900 Installation and Setup Instructions](#)

### Video steps - AFF A900

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

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

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

[Animation - AFF A900 Installation and setup instructions](#)

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

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

 | <https://img.youtube.com/vi/WAE0afWhj1c/?maxresdefault.jpg>

Detailed steps - AFF 900

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

Step 1: Prepare for installation

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

Before you begin

You need to have access to the [NetApp Hardware Universe](#) for information about site requirements as well as additional information on your configured system.

You might also want to have access to the [ONTAP 9 Release Notes](#) for your version of ONTAP for more information about this system.

You need to provide the following at your site:

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

Steps

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



3. Inventory and make a note of the number and types of cables you received.

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

[NetApp Hardware Universe](#)

Type of cable...	Part number and length	Connector type	For...
25 GbE data Cable	X66240A-05 (112-00639), 0.5m		Network cable
	X66240A-2 (112-00598), 2m		
	X66240A-5 (112-00600), 5m		

Type of cable...	Part number and length	Connector type	For...
32 Gb FC (SFP+ Op)	X66250-2 (112-00342), 2m X66250-5 (112-00344), 5m X66250-15 (112-00346), 15m		FC optical network cable
40 GbE network cable	X66100-1 (112-00542), 1m X66100-3 (112-00543), 3m X66100-5 (112-00544), 5m		Ethernet data, cluster network
100 GbE cable	X66211B-1 (112-00573), 1m X66211B-2 (112-00574), 2m X66211B-5 (112-00576), 5m		Network, NVME storage, Ethernet data, cluster network
Optical cables	X66031A (112-00436), 1m X66032A (112-00437), 2m X66033A (112-00438), 3m		FC optical network
Cat 6, RJ-45 (order dependent)	Part numbers X6585-R6 (112-00291), 3m X6562-R6 (112-00196), 5m		Management network and Ethernet data
Micro-USB console cable	Not applicable		Console connection during software setup on non-Windows or Mac laptop/console
Power cables	Not applicable		Powering up the system

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

## Step 2: Install the hardware

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

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



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



3. Attach cable management devices (as shown).



4. Place the bezel on the front of the system.

### Step 3: Cable controllers to your network

You can cable the controllers to your network by using the two-node switchless cluster method or by using the cluster interconnect network.

#### Option 1: Two-node switchless cluster

Management network, data network, and management ports on the controllers are connected to switches. The cluster interconnect ports are cabled on both controllers.

#### Before you begin

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

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all networking module ports.







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

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

#### Animation - Cable a two-node switchless cluster



Step	Perform on each controller
1	<p>Cable cluster interconnect ports:</p> <ul style="list-style-type: none"><li>• Slot A4 and B4 (e4a)</li><li>• Slot A8 and B8 (e8a)</li></ul> 
2	<p>Cable controller management (wrench) ports.</p> 

Step	Perform on each controller
3	<p>Cable 25 GbE network switches:</p> <p>Ports in slot A3 and B3 (e3a and e3c) and slot A9 and B9 (e9a and e9c) to the 25 GbE network switches.</p>  <p>40GbE host network switches:</p> <p>Cable host-side b ports in slot A4 and B4 (e4b) and slot A8 and B8 (e8b) to the host switch.</p> 
4	<p>Cable 32 Gb FC connections:</p> <p>Cable ports in slot A5 and B5 (5a, 5b, 5c, and 5d) and slot A7 and B7 (7a, 7b, 7c, and 7d) to the 32 Gb FC network switches.</p> 

2. To cable your storage, see [Step 4: Cable controllers to drive shelves](#).

#### Option 2: Switched cluster

Management network, data network, and management ports on the controllers are connected to switches. The cluster interconnect and HA ports are cabled on to the cluster/HA switch.

#### Before you begin

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

Be sure to check the direction of the cable pull-tabs when inserting the cables in the ports. Cable pull-tabs are up for all networking module ports.



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

1. Use the animation or illustration to complete the cabling between the controllers and to the switches:

[Animation - Cable a switched cluster](#)





Step	Perform on each controller
1	<p>Cable cluster interconnect a ports:</p> <ul style="list-style-type: none"> <li>Slot A4 and B4 (e4a) to the cluster network switch.</li> <li>Slot A8 and B8 (e8a) to the cluster network switch.</li> </ul> 
2	<p>Cable controller management (wrench) ports.</p> 

Step	Perform on each controller
3	<p>Cable 25GbE network switches:</p> <p>Ports in slot A3 and B3 (e3a and e3c) and slot A9 and B9 (e9a and e9c) to the 25 GbE network switches.</p>  <p>40GbE host network switches:</p> <p>Cable host-side b ports in slot A4 and B4 (e4b) and slot A8 and B8 (e8b) to the host switch.</p> 
4	<p>Cable 32 Gb FC connections:</p> <p>Cable ports in slot A5 and B5 (5a, 5b, 5c, and 5d) and slot A7 and B7 (7a, 7b, 7c, and 7d) to the 32 Gb FC network switches.</p> 

2. To cable your storage, see [Step 4: Cable controllers to drive shelves](#).

#### Step 4: Cable controllers to drive shelves

##### Option 1: Cable the controllers to a single NS224 drive shelf in AFF A900

You must cable each controller to the NSM modules on the NS224 drive shelf on an AFF A900 system.

##### Before you begin

- Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the storage modules are up, while the pull tabs on the shelves are down.





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

1. Use the following animation or drawings to cable your controllers to a single NS224 drive shelf.

#### Animation - Cable a single NS224 shelf



Step	Perform on each controller
1	<ul style="list-style-type: none"><li>• Connect controller A port e2a to port e0a on NSM A on the shelf.</li><li>• Connect controller A port e10b to port e0b on NSM B on the shelf.</li></ul>  100 GbE cable

Step	Perform on each controller
2	<ul style="list-style-type: none"> <li>Connect controller B port e2a to port e0a on NSM B on the shelf.</li> <li>Connect controller B port e10b to port e0b on NSM A on the shelf.</li> </ul>  <p>100 GbE cable</p>

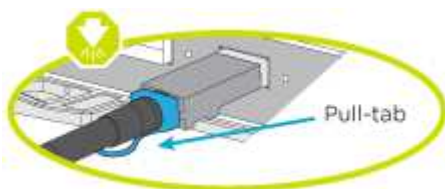
- To complete setting up your system, see [Step 5: Complete system setup and configuration](#).

#### Option 2: Cable the controllers to two NS224 drive shelves in AFF A900

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

#### Before you begin

- Be sure to check the illustration arrow for the proper cable connector pull-tab orientation. The cable pull-tab for the storage modules are up, while the pull tabs on the shelves are down.



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

- Use the following animation or diagram to cable your controllers to two NS224 drive shelves.

[Animation - Cable two NS224 shelves](#)



Step	Perform on each controller
<div data-bbox="183 159 245 197" style="background-color: #005596; color: white; padding: 2px 5px; display: inline-block;">1</div>	<ul style="list-style-type: none"> <li>• Connect controller A port e2a to NSM A e0a on shelf 1.</li> <li>• Connect controller A port e10b to NSM B e0b on shelf 1.</li> <li>• Connect controller A port e2b to NSM B e0b on shelf 2.</li> <li>• Connect controller A port e10a to NSM A e0a on shelf 2.</li> </ul> <div data-bbox="889 514 1092 546" style="text-align: center;">  </div> <p style="text-align: center;">100 GbE cable</p>
<div data-bbox="183 678 245 716" style="background-color: #FFB300; color: white; padding: 2px 5px; display: inline-block;">2</div>	<ul style="list-style-type: none"> <li>• Connect controller B port e2a to NSM B e0a on shelf 1.</li> <li>• Connect controller B port e10b to NSM A e0b on shelf 1.</li> <li>• Connect controller B port e2b to NSM A e0b on shelf 2.</li> <li>• Connect controller B port e10a to NSM B e0a on shelf 2.</li> </ul> <div data-bbox="841 1031 1044 1062" style="text-align: center;">  </div> <p style="text-align: center;">100 GbE cable</p>

2. To complete setting up your system, see [Step 5: Complete system setup and configuration](#).

### Step 5: Complete system setup and configuration

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

#### Option 1: If network discovery is enabled

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

1. Use the following animation or drawing to set one or more drive shelf IDs:

The NS224 shelves are pre-set to shelf ID 00 and 01. If you want to change the shelf IDs, you must create a tool to insert into the hole where button is located.

[Animation - Set SAS or NVMe drive shelf IDs](#)





1	Remove the end cap.
2	Press and hold shelf ID button until first digit blinks, then push to advance to 0-9.  Note: The first digit continues to blink
3	Press and hold shelf ID button until second digit blinks, then push to advance to 0-9. Note: The first digit stops blinking, and the second digit continues to blink.
4	Replace the end cap.
5	Wait 10 seconds for the Amber LED (!) to appear, then power-cycle the drive shelf to set shelf ID.

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
3. Turn on the power switches to both nodes.

[Animation - Turn on the power to the controllers](#)



Initial booting may take up to eight minutes.

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

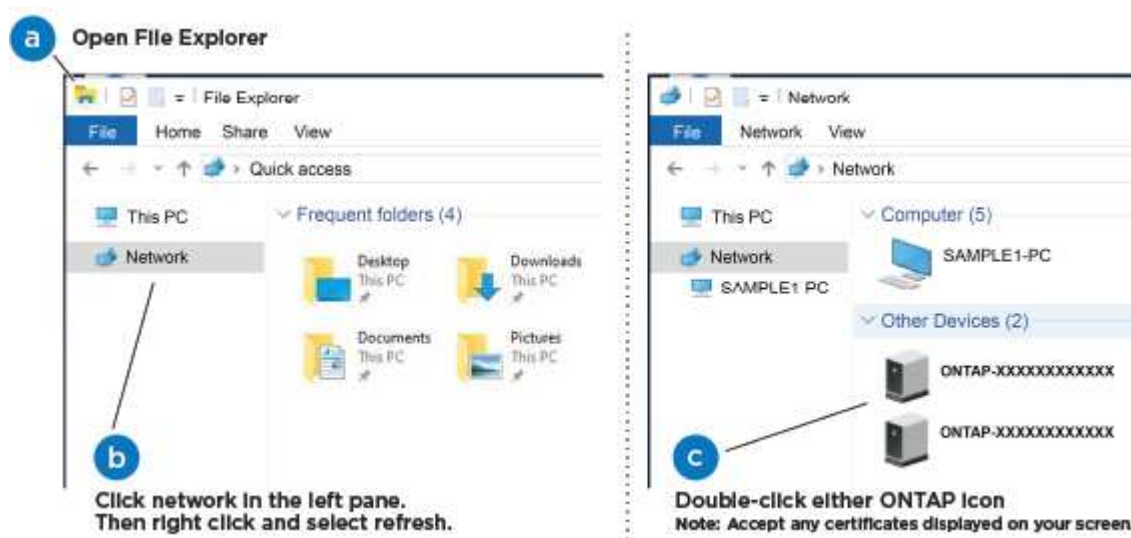
See your laptop's online help for more information.

5. Use the following animation to connect your laptop to the Management switch.

[Animation - Connect your laptop to the Management switch](#)



6. Select an ONTAP icon listed to discover:



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



XXXXX is the system serial number for the target node.

System Manager opens.

7. Use System Manager guided setup to configure your system using the data you collected in the [ONTAP Configuration Guide](#).
8. Set up your account and download Active IQ Config Advisor:
  - a. Log in to your existing account or create an account.

[NetApp Support Registration](#)



- b. Register your system.

[NetApp Product Registration](#)

- c. Download Active IQ Config Advisor.

[NetApp Downloads: Config Advisor](#)

9. Verify the health of your system by running Config Advisor.
10. After you have completed the initial configuration, go to the [ONTAP & ONTAP System Manager Documentation Resources](#) page for information about configuring additional features in ONTAP.

#### Option 2: If network discovery is not enabled

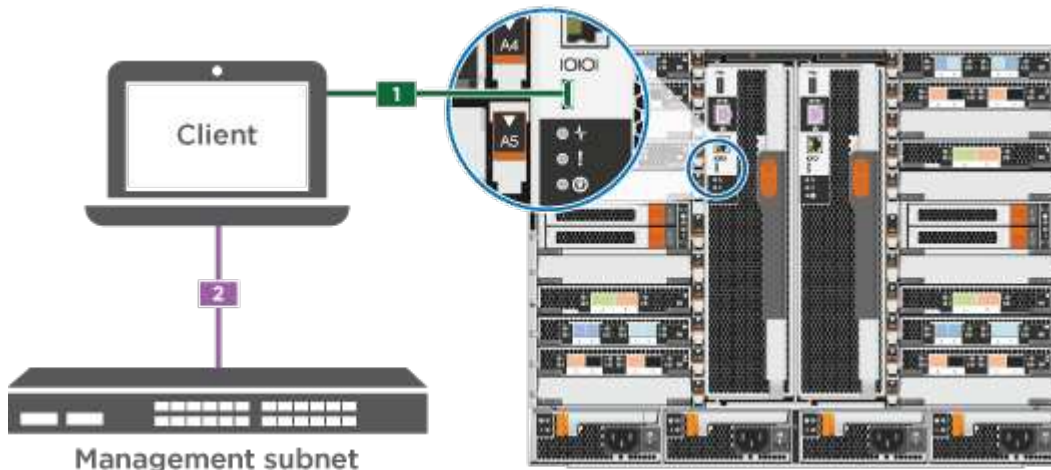
If you are not using a Windows or Mac-based laptop or console or if auto discovery is not enabled, you must complete the configuration and setup using this task.

1. Cable and configure your laptop or console:
  - a. Set the console port on the laptop or console to 115,200 baud with N-8-1.



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

- b. Connect the console cable to the laptop or console using the console cable that came with your system, and then connect the laptop to the management switch on the management subnet.



- c. Assign a TCP/IP address to the laptop or console, using one that is on the management subnet.
2. Use the following animation to set one or more drive shelf IDs:

The NS224 shelves are pre-set to shelf ID 00 and 01. If you want to change the shelf IDs, you must create a tool to insert into the hole where button is located.

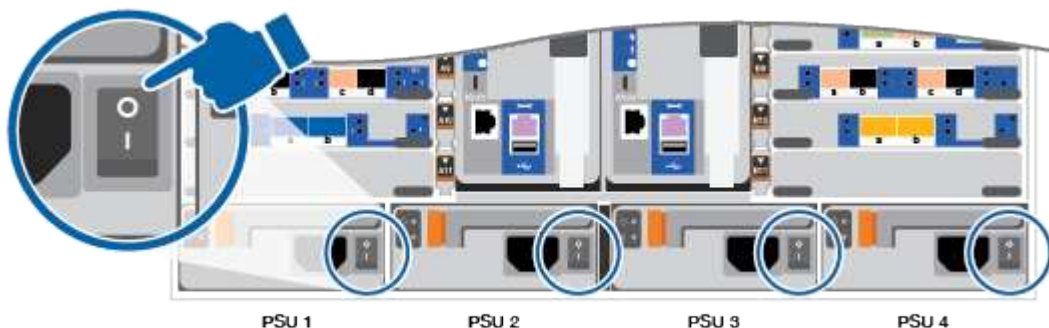
[Animation - Set SAS or NVMe drive shelf IDs](#)



1	Remove the end cap.
2	Press and hold shelf ID button until first digit blinks, then push to advance to 0-9.  Note: The first digit continues to blink
3	Press and hold shelf ID button until second digit blinks, then push to advance to 0-9. Note: The first digit stops blinking, and the second digit continues to blink.
4	Replace the end cap.
5	Wait 10 seconds for the Amber LED (!) to appear, then power-cycle the drive shelf to set shelf ID.

3. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.
4. Turn on the power switches to both nodes.

[Animation - Turn on the power to the controllers](#)



Initial booting may take up to eight minutes.

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

2. Using System Manager on your laptop or console, configure your cluster:

- a. Point your browser to the node management IP address.



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

- b. Configure the system using the data you collected in the *NetApp ONTAP Configuration guide*.

[ONTAP Configuration Guide](#)

3. Set up your account and download Active IQ Config Advisor:

- a. Log in to your existing account or create an account.

[NetApp Support Registration](#)

- b. Register your system.

[NetApp Product Registration](#)

- c. Download Active IQ Config Advisor.

[NetApp Downloads: Config Advisor](#)

4. Verify the health of your system by running Config Advisor.
5. After you have completed the initial configuration, go to the [ONTAP & ONTAP System Manager Documentation Resources](#) page for information about configuring additional features in ONTAP.

## Maintain

### Add an I/O module - AFF A900

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

## Before you begin

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

## Option 1: Add the I/O module to a system with open slots

You can add an I/O module into an empty module slot in your system as either a NIC or a storage module for the NS224 storage shelves.

### 1. Shutdown controller A:

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

The console connection shows that the controller drops to the LOADER prompt when the take over is complete.

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

### 3. Remove the target slot blanking cover:

- Depress the lettered and numbered cam button.
- Rotate the cam latch down until it is the open position.
- Remove the blanking cover.

### 4. Install the I/O module:

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

### 5. If the replacement I/O module is a NIC, cable the module to the data switches.



Make sure that any unused I/O slots have blanks installed to prevent possible thermal issues.

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

### 7. Give back the controller from the partner controller. `storage failover giveback -ofnode target_node_name`

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

### 9. If you are using slots 3 and/or 7 for networking, use the `storage port modify -node <node name> -port <port name> -mode network` command to convert the slot for networking use.

10. Repeat these steps for controller B.
11. If you installed a storage I/O module, install and cable your NS224 shelves, as described in [Hot-adding an NS224 drive shelf](#).

## Option 2: Add an I/O module in a system with no open slots

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

1. If you are:

Replacing a...	Then...
NIC I/O module with the same the same number of ports	The LIFs will automatically migrate when its controller module is shut down.
NIC I/O module with fewer ports	Permanently reassign the affected LIFs to a different home port. See <a href="#">Migrating a LIF</a> for information about using System Manager to permanently move the LIFs.
NIC I/O module with a storage I/O module	Use System Manager to permanently migrate the LIFs to different home ports, as described in <a href="#">Migrating a LIF</a> .

2. Shut down controller A:

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

The console connection shows that the controller drops to the LOADER prompt when the take over is complete.

3. If you are not already grounded, properly ground yourself.
4. Unplug any cabling on the target I/O module.
5. Remove the target I/O module from the chassis:

- a. Depress the lettered and numbered cam button.

The cam button moves away from the chassis.

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

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

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

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

[Animation - Remove or replacing an I/O module](#)



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

6. Install the I/O module into the target slot:
  - a. Align the I/O module with the edges of the slot.
  - b. Slide the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin.
  - c. Push the I/O cam latch all the way up to lock the module in place.
7. Repeat the remove and install steps to replace additional modules for controller A.
8. If the replacement I/O module is a NIC, cable the module or modules to the data switches.
9. Reboot the controller from the LOADER prompt: `bye`
10. Give back the controller from the partner controller. `storage failover giveback -ofnode target_node_name`
11. Enable automatic giveback if it was disabled: `storage failover modify -node local -auto -giveback true`
12. If you added:

If I/O module is a...	Then...
NIC module in slots 3 or 7,	Use the <code>storage port modify -node *<i>&lt;node name&gt;</i> -port *<i>&lt;port name&gt;</i> -mode network</code> command for each port.
Storage module	Install and cable your NS224 shelves, as described in <a href="#">Hot-adding an NS224 drive shelf</a> .

13. Repeat these steps for controller B.

## Boot media

### Replace the boot media - AFF A900

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

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

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

- The nondisruptive and disruptive methods for replacing a boot media both require you to restore the `var` file system:
  - For nondisruptive replacement, the HA pair does not require connection to a network to restore the `var` file system. The HA pair in a single chassis has an internal e0S connection, which is used to transfer `var` config between them.
  - For disruptive replacement, you do not need a network connection to restore the `var` file system, but the process requires two reboots.
- You must replace the failed component with a replacement FRU component you received from your provider.
- It is important that you apply the commands in these steps on the correct controller:
  - The *impaired* controller is the controller on which you are performing maintenance.
  - The *healthy* controller is the HA partner of the impaired controller.

### Pre-shutdown checks for onboard encryption keys - AFF A900

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

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

### Steps

1. Check the status of the impaired controller:

- If the impaired controller is at the login prompt, log in as `admin`.
- If the impaired controller is at the `LOADER` prompt and is part of HA configuration, log in as `admin` on the healthy controller.
- If the impaired controller is in a standalone configuration and at `LOADER` prompt, contact [mysupport.netapp.com](https://mysupport.netapp.com).

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

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

The following AutoSupport message suppresses automatic case creation for two hours: `cluster1:*>`  
`system node autosupport invoke -node * -type all -message MAINT=2h`

3. Check the version of ONTAP the system is running on the impaired controller if up, or on the partner controller if the impaired controller is down, using the `version -v` command:

- If `<Ino-DARE>` or `<1Ono-DARE>` is displayed in the command output, the system does not support NVE, proceed to shut down the controller.

### ONTAP 9.6 and later

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

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

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

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

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

### Verify NVE configuration

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



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

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



yes, you need to complete some additional steps.

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

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

3. If the `Key Manager` type displays `external` and the `Restored` column displays anything other than `yes`:
  - a. Restore the external key management authentication keys to all nodes in the cluster: `security key-manager external restore`

If the command fails, contact NetApp Support.

[mysupport.netapp.com](https://mysupport.netapp.com)

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



Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support. [mysupport.netapp.com](https://mysupport.netapp.com)

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

## Verify NSE configuration

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



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

- If the Key Manager type displays `external` and the Restored column displays `yes`, it's safe to shut down the impaired controller.
  - If the Key Manager type displays `onboard` and the Restored column displays `yes`, you need to complete some additional steps.
  - If the Key Manager type displays `external` and the Restored column displays anything other than `yes`, you need to complete some additional steps.
  - If the Key Manager type displays `external` and the Restored column displays anything other than `yes`, you need to complete some additional steps.
2. If the Key Manager type displays `onboard` and the Restored column displays `yes`, manually back up the OKM information:
    - a. Go to advanced privilege mode and enter `y` when prompted to continue: `set -priv advanced`
    - b. Enter the command to display the key management information: `security key-manager onboard show-backup`
    - c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM.
    - d. Return to admin mode: `set -priv admin`
    - e. You can safely shut down the controller.
  3. If the Key Manager type displays `external` and the Restored column displays anything other than `yes`:
    - a. Enter the onboard security key-manager sync command: `security key-manager external sync`  
  
If the command fails, contact NetApp Support.  
  
[mysupport.netapp.com](https://mysupport.netapp.com)
    - b. Verify that the Restored column equals `yes` for all authentication keys: `security key-manager key-query`
    - c. You can safely shut down the controller.
  4. If the Key Manager type displays `onboard` and the Restored column displays anything other than `yes`:
    - a. Enter the onboard security key-manager sync command: `security key-manager onboard sync`  
  
Enter the customer's onboard key management passphrase at the prompt. If the passphrase cannot be provided, contact NetApp Support.  
  
[mysupport.netapp.com](https://mysupport.netapp.com)

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

### **Shut down the impaired controller - AFF A900**

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

## Most configurations

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

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

### About this task

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

#### [ONTAP 9 NetApp Encryption Power Guide](#)

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

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

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the [Administration overview with the CLI](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

### Steps

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

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

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

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

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

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

If the impaired controller is displaying...	Then...
System prompt or password prompt (enter system password)	<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 <code>y</code>.</p>

### Controller is in a MetroCluster

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



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

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

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the [Administration overview with the CLI](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

### Steps

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

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

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

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

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

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

If the impaired controller is displaying...	Then...
System prompt or password prompt (enter system password)	<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 <code>y</code>.</p>

## Remove the controller, replace the boot media, and transfer the boot image - AFF A900

You must remove and open the controller module, locate and replace the boot media in the controller, and then transfer the image to the replacement boot media.

### Step 1: Remove the controller module

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

#### Steps

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

[Animation - Remove the controller](#)



1	Cam handle release button
2	Cam handle

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

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

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



1	Controller module cover locking button
---	--

## Step 2: Replace the boot media

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

### Steps

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

[Animation - Replace boot media](#)





1	Press release tab
2	Boot media

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



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

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

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

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

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

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

#### Before you begin

- You must have a USB flash drive, formatted to FAT32, with at least 4GB capacity.
- A copy of the same image version of ONTAP as what the impaired controller was running. You can download the appropriate image from the Downloads section on the NetApp Support Site
  - If NVE is enabled, download the image with NetApp Volume Encryption, as indicated in the download button.
  - If NVE is not enabled, download the image without NetApp Volume Encryption, as indicated in the download button.
- If your system is a stand-alone system you do not need a network connection, but you must perform an additional reboot when restoring the var file system.

#### Steps

1. Align the end of the controller module with the opening in the chassis, and then gently push the controller module halfway into the system.
2. Recable the controller module, as needed.
3. Insert the USB flash drive into the USB slot on the controller module.

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

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

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

5. Interrupt the boot process to stop at the LOADER prompt by pressing Ctrl-C when you see Starting AUTOBOOT press Ctrl-C to abort....

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

6. Set your network connection type at the LOADER prompt:
  - If you are configuring DHCP: `ifconfig e0a -auto`



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

◦ If you are configuring manual connections: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`

- `filer_addr` is the IP address of the storage system.
- `netmask` is the network mask of the management network that is connected to the HA partner.
- `gateway` is the gateway for the network.
- `dns_addr` is the IP address of a name server on your network.
- `dns_domain` is the Domain Name System (DNS) domain name.

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



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

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

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

The changes will be implemented when the system is booted.

## Boot the recovery image - AFF A900

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

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

The image is downloaded from the USB flash drive.

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

If your system has...	Then...
A network connection	<ul style="list-style-type: none"> <li>a. Press <code>y</code> when prompted to restore the backup configuration.</li> <li>b. Press <code>y</code> when prompted to overwrite <code>/etc/ssh/ssh_host_ecdsa_key</code>.</li> <li>c. Press <code>y</code> when prompted to confirm if the restore backup was successful.</li> <li>d. Press <code>y</code> when prompted to the restored configuration copy.</li> <li>e. Set the impaired controller to advanced privilege level: <code>set -privilege advanced</code></li> <li>f. Run the restore backup command: <code>system node restore-backup -node local -target-address impaired_node_IP_address</code></li> <li>g. Return the impaired controller to admin level: <code>set -privilege admin</code></li> <li>h. Press <code>y</code> when prompted to use the restored configuration.</li> <li>i. Press <code>y</code> when prompted to reboot the impaired controller.</li> </ul>
No network connection	<ul style="list-style-type: none"> <li>a. Press <code>n</code> when prompted to restore the backup configuration.</li> <li>b. Reboot the system when prompted by the system.</li> <li>c. Select the <b>Update flash from backup config</b> (sync flash) option from the displayed menu.</li> </ul> <p>If you are prompted to continue with the update, press <code>y</code>.</p>

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

4. Ensure that the environmental variables are set as expected:
  - a. Take the impaired controller to the LOADER prompt.
  - b. Check the environment variable settings with the `printenv` command.
  - c. If an environment variable is not set as expected, modify it with the `setenv environment_variable_name changed_value` command.
  - d. Save your changes using the `saveenv` command.
5. The next depends on your system configuration:
  - If your system has onboard keymanager, NSE or NVE configured, go to [Post boot media replacement steps for OKM, NSE, and NVE](#)

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

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

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

7. Connect the console cable to the partner controller.

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

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

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

10. Move the console cable to the repaired Shut down or take over the impaired controller using the appropriate procedure for your configuration. and run the `version -v` command to check the ONTAP versions.

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

## Post boot media replacement steps for OKM, NSE, and NVE - AFF A900

Once environment variables are checked, you must complete steps specific to restore Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) and NetApp Volume Encryption (NVE).

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

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

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

If the console displays...	Then...
The LOADER prompt	Boot the controller to the boot menu: <code>boot_ontap menu</code>

If the console displays...	Then...
Waiting for giveback....	<ol style="list-style-type: none"> <li>Enter <code>Ctrl-C</code> at the prompt</li> <li>At the message: Do you wish to halt this node rather than wait [y/n]? , enter: <code>y</code></li> <li>At the LOADER prompt, enter the <code>boot_ontap</code> menu command.</li> </ol>

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



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

Example of backup data:

Enter the backup data:

```
-----BEGIN BACKUP-----
TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
QAAAAAAAAABvOIH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TIYFss4PDjTaV
dzRYkLd1PhQLxAWJwOlyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAACgAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAA
lgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAACAAAAAAJAGr3tJA/
LRzUQRHwv+1aWvAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBf
ml4NBsSyV1B4jc4A7cvWEFY6ILG6hc6tbKLAHZuvfQ4rlbYAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAA
-----END BACKUP-----
```

- At the Boot Menu select the option for Normal Boot.  
The system boots to Waiting for giveback... prompt.
- Move the console cable to the partner controller and log in as admin.
- Confirm the target controller is ready for giveback with the `storage failover show` command.
- Give back only the CFO aggregates with the `storage failover giveback -fromnode local -only-cfo-aggregates true` command.
  - If the command fails because of a failed disk, physically disengage the failed disk, but leave the disk in

the slot until a replacement is received.

- If the command fails because of an open CIFS session, check with the customer how to close out CIFS sessions.



Terminating CIFS can cause loss of data.

- If the command fails because the partner "not ready", wait 5 minutes for the NVRAMs to synchronize.
- If the command fails because of an NDMP, SnapMirror, or SnapVault process, disable the process. See the appropriate content for more information.

11. Once the giveback completes, check the failover and giveback status with the `storage failover show` and `storage failover show-giveback` commands.

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

12. If you are running ONTAP 9.6 or later, run the security key-manager onboard sync:

- a. Run the `security key-manager onboard sync` command and then enter the passphrase when prompted.
- b. Enter the `security key-manager key-query` command to see a detailed view of all keys stored in the onboard key manager and verify that the `Restored` column = `yes/true` for all authentication keys.



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

- c. Wait 10 minutes for the key to synchronize across the cluster.

13. Move the console cable to the partner controller.

14. Give back the target controller using the `storage failover giveback -fromnode local` command.

15. Check the giveback status, three minutes after it reports complete, using the `storage failover show` command.

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

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

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

17. Move the console cable to the target controller and run the `version -v` command to check the ONTAP versions.

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

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

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



If the console displays...	Then...
The login prompt	Go to step 7.
Waiting for giveback...	<ul style="list-style-type: none"> <li>a. Log into the partner controller.</li> <li>b. Confirm the target controller is ready for giveback with the <code>storage failover show</code> command.</li> </ul>

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



Terminating CIFS can cause loss of data.

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

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

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



If the command fails, contact Customer Support.

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

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

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

## Return the failed part to NetApp - AFF A900

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

## Chassis

### Replace the chassis - AFF A900

#### Before you begin

To replace the chassis, you must remove the power supplies, fans, controller modules, I/O modules, DCPM modules, and USB LED module from the impaired chassis, remove the impaired chassis from the equipment rack or system cabinet, install the replacement chassis in its place, and then install the components into the replacement chassis.

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

#### About this task

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

### Shutdown the impaired controller - AFF A900

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

#### About this task

- If you have a cluster with more than two controllers, it must be in quorum. If the cluster is not in quorum or a healthy controller shows `false` for eligibility and health, you must correct the issue before shutting down the impaired controller; see the [Administration overview with the CLI](#).
- If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:  

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

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

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

## Steps

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

If your system is running clustered ONTAP with...	Then...
Two controllers in the cluster	<code>cluster ha modify -configured false storage failover modify -node node0 -enabled false</code>
More than two controllers in the cluster	<code>storage failover modify -node node0 -enabled false</code>

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

The confirmation message looks like the following:

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

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



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

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

Answer `y` when prompted.

## Move and replace hardware - AFF A900

To replace the chassis, you must remove the components from the old chassis and install them in the replacement chassis.

### Step 1: Remove the power supplies

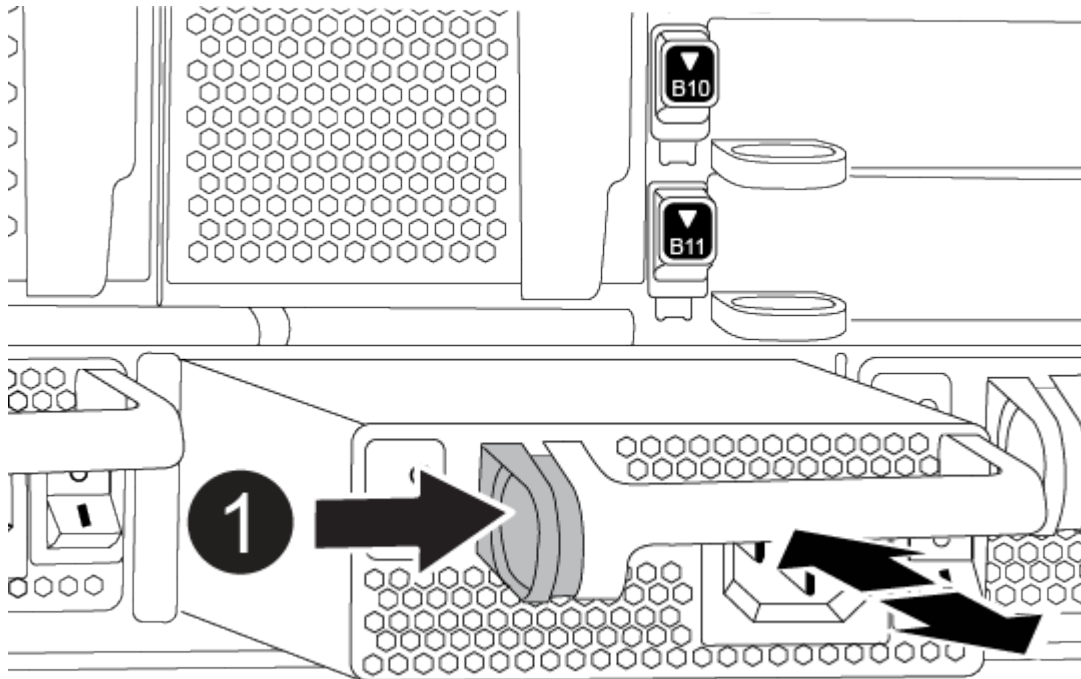
Removing the power supplies when replacing a chassis involves turning off, disconnecting, and then removing the power supply from the old chassis.

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



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

#### Animation - Remove/install PSU



1

Locking button

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

#### Step 2: Remove the fans

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

1. If you are not already grounded, properly ground yourself.
2. Remove the bezel (if necessary) with two hands, by grasping the openings on each side of the bezel, and then pulling it toward you until the bezel releases from the ball studs on the chassis frame.
3. Press the terra cotta button on the fan module and pull the fan module straight out of the chassis, making sure that you support it with your free hand.



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

#### Animation - Remove/install fan



1	Orange release button
2	Slide fan in/out of chassis

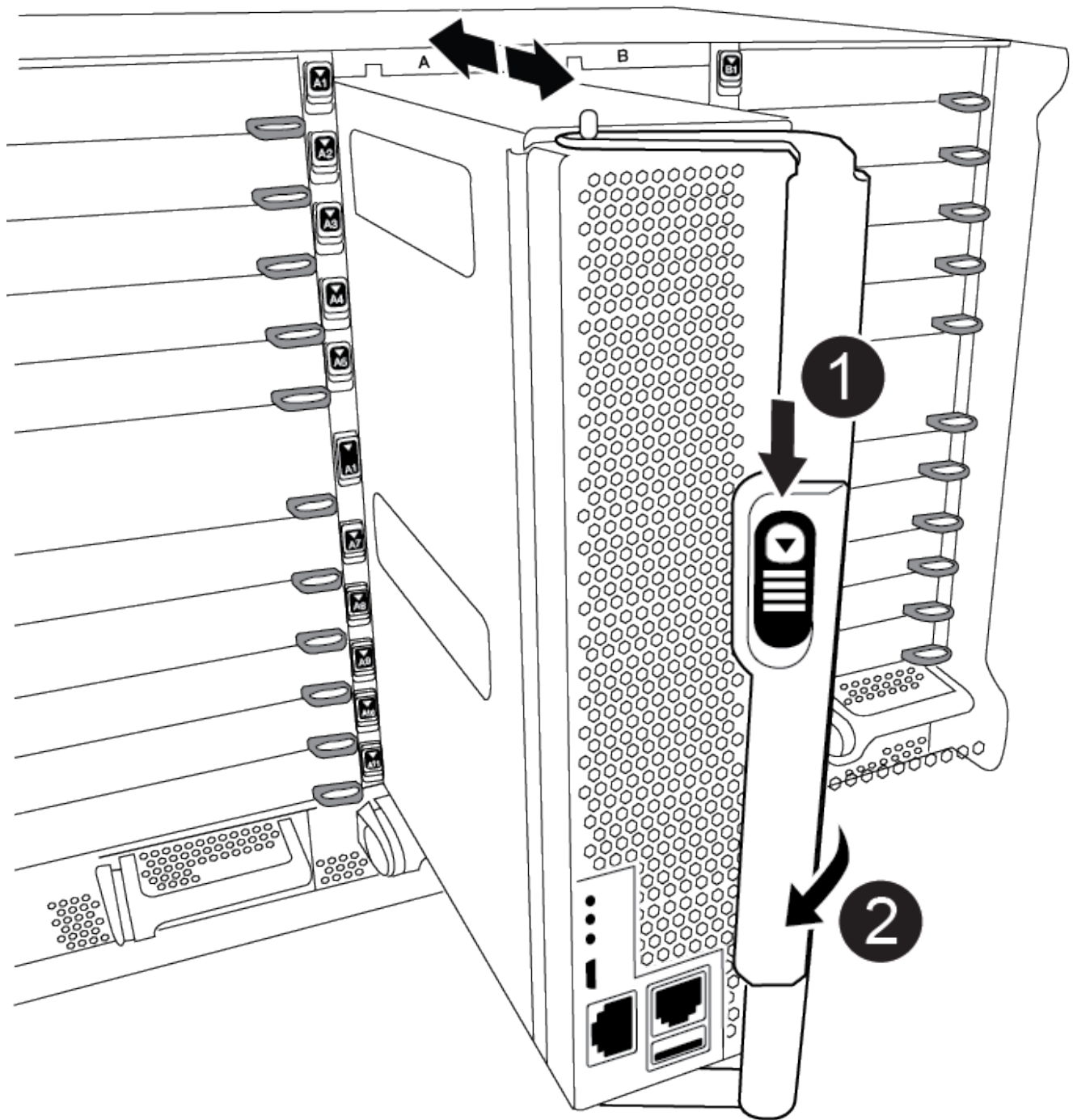
4. Set the fan module aside.
5. Repeat the preceding steps for any remaining fan modules.

#### Step 3: Remove the controller module

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

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

#### Animation - Remove the controller



1	Cam handle release button
2	Cam handle

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

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

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

#### **Step 4: Remove the I/O modules**

To remove I/O modules from the old chassis, including the NVRAM modules, follow the specific sequence of steps. You do not have to remove the FlashCache module, if present, from the NVRAM module when moving it to a new chassis.

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

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

3. Remove the target I/O module from the chassis:
  - a. Depress the lettered and numbered cam button.

The cam button moves away from the chassis.

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

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

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

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

[Animation - Remove/install I/O module](#)



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

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

#### Step 5: Remove the De-stage Controller Power Module

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

1. If you are not already grounded, properly ground yourself.
2. Press the terra cotta locking button on the module handle, and then slide the DCPM module out of the chassis.

[Animation - Remove/install DCPM](#)





1

DCPM module terra cotta locking button

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

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

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

1. Remove the screws from the chassis mount points.



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

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

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

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

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

#### Animation - Remove/install USB



1	Eject the module.
2	Slide out of chassis.

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

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

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

1. If you are not already grounded, properly ground yourself.
2. Align the end of the DCPM module with the chassis opening, and then gently slide it into the chassis until it clicks into place.



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

3. Repeat this step for the remaining DCPM module.

### Step 9: Install fans into the chassis

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

1. If you are not already grounded, properly ground yourself.
2. Align the edges of the replacement fan module with the opening in the chassis, and then slide it into the chassis until it snaps into place.

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

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

### Step 10: Install I/O modules

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

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

1. If you are not already grounded, properly ground yourself.
2. After the replacement chassis is installed in the rack or cabinet, install the I/O modules into their corresponding slots in the replacement chassis by gently sliding the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage, and then push the I/O cam latch all the way up to lock the module in place.
3. Recable the I/O module, as needed.
4. Repeat the preceding step for the remaining I/O modules that you set aside.



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

### Step 11: Install the power supplies

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

1. If you are not already grounded, properly ground yourself.
2. Using both hands, support and align the edges of the power supply with the opening in the system chassis, and then gently push the power supply into the chassis until it locks into place.

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



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

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



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

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

### Step 12: Install the controller

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

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



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

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



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

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

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



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

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

## Restore and verify the configuration - AFF C190

To complete the chassis replacement, you must complete specific tasks.

### Step 1: Verifying and setting the HA state of the chassis

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

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

The HA state should be the same for all components.

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

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

- `ha`
- `non-ha`

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

### Step 2: Run system-level diagnostics

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

#### Before you begin

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

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

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

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



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

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



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

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

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

4. Enable the interconnect diagnostics tests from the Maintenance mode prompt: `sldiag device modify -dev interconnect -sel enable`

The interconnect tests are disabled by default and must be enabled to run separately.

5. Run the interconnect diagnostics test from the Maintenance mode prompt: `sldiag device run -dev interconnect`

You only need to run the interconnect test from one controller.

6. Verify that no hardware problems resulted from the replacement of the chassis: `sldiag device status -dev interconnect -long -state failed`

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

7. Proceed based on the result of the preceding step.

If the system-level diagnostics tests...	Then...
Were completed without any failures	<div><div>a. Clear the status logs: <code>sldiag device clearstatus</code></div><div>b. Verify that the log was cleared: <code>sldiag device status</code></div><div>The following default response is displayed:</div><div><div>SLDIAG: No log messages are present.</div></div><div>c. Exit Maintenance mode on both controllers: <code>halt</code></div><div>The system displays the LOADER prompt.</div><div><div></div><div>You must exit Maintenance mode on both controllers before proceeding any further.</div></div><div>d. Enter the following command on both controllers at the LOADER prompt: <code>bye</code></div><div>e. Return the controller to normal operation.</div></div>

If your system is running ONTAP...	Then...
With two nodes in the cluster	Issue these commands: <pre>node::&gt; cluster ha modify -configured true`node::&gt; storage failover modify -node node0 -enabled true</pre>
With more than two nodes in the cluster	Issue this command: <pre>node::&gt; storage failover modify -node node0 -enabled true</pre>
In a stand-alone configuration	You have no further steps in this particular task. You have completed system-level diagnostics.
Resulted in some test failures	Determine the cause of the problem. <ol style="list-style-type: none"> <li>Exit Maintenance mode: <code>halt</code></li> <li>Perform a clean shutdown, and then disconnect the power supplies.</li> <li>Verify that you have observed all of the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.</li> <li>Reconnect the power supplies, and then power on the storage system.</li> <li>Rerun the system-level diagnostics test.</li> </ol>

### Step 3: Return the failed part to NetApp

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

## Controller module

### Replace the controller module - AFF A900

To replace the impaired controller module, you must shut down the impaired controller, move the internal components to the replacement controller module, install the replacement controller module, and reboot the replacement controller.

#### Before you begin

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

- All drive shelves must be working properly.
- If your system is a FlexArray system or has a V\_StorageAttach license, you must refer to the additional required steps before performing this procedure.

- If your system is in an HA pair, the healthy controller must be able to take over the controller that is being replaced (referred to in this procedure as the “impaired controller”).
- If your system is in a MetroCluster configuration, you must review the section [Choosing the correct recovery procedure](#) to determine whether you should use this procedure.

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

- You must replace the failed component with a replacement FRU component you received from your provider.
- You must be replacing a controller module with a controller module of the same model type. You cannot upgrade your system by just replacing the controller module.
- You cannot change any drives or drive shelves as part of this procedure.
- In this procedure, the boot device is moved from the impaired controller to the replacement controller so that the replacement controller will boot up in the same version of ONTAP as the old controller module.
- It is important that you apply the commands in these steps on the correct systems:
  - The impaired controller is the controller that is being replaced.
  - The replacement controller is the new controller that is replacing the impaired controller.
  - The healthy controller is the surviving controller.
- You must always capture the controller’s console output to a text file.

This provides you a record of the procedure so that you can troubleshoot any issues that you might encounter during the replacement process.

### **Shut down the impaired controller - AFF A900**

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



## Option 1: Most systems

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

### About this task

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

#### [ONTAP 9 NetApp Encryption Power Guide](#)

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

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

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the [Administration overview with the CLI](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

### Steps

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

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

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

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

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

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to Remove controller module.
Waiting for giveback...	Press Ctrl-C, and then respond <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: <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 <code>y</code>.</p>

## Option 2: Controller is in a MetroCluster



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

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

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the [Administration overview with the CLI](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

### Steps

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

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

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

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

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

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to Remove controller module.
Waiting for giveback...	Press Ctrl-C, and then respond <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: <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 <code>y</code>.</p>

## Replace the controller module hardware - AFF A900

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

The following animation shows the whole process of moving components from the impaired to the replacement

controller.

[Animation - Move components to replacement controller](#)

**Step 1: Remove the controller module**

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

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

[Animation - Remove the controller](#)



1	Cam handle release button
2	Cam handle

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

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

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



1

Controller module cover locking button

#### Step 2: Move the boot media

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

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



1	Press release tab
2	Boot media

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



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

3. Move the boot media to the new controller module, align the edges of the boot media with the socket housing, and then gently push it into the socket.
4. Check the boot media to make sure that it is seated squarely and completely in the socket.

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

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

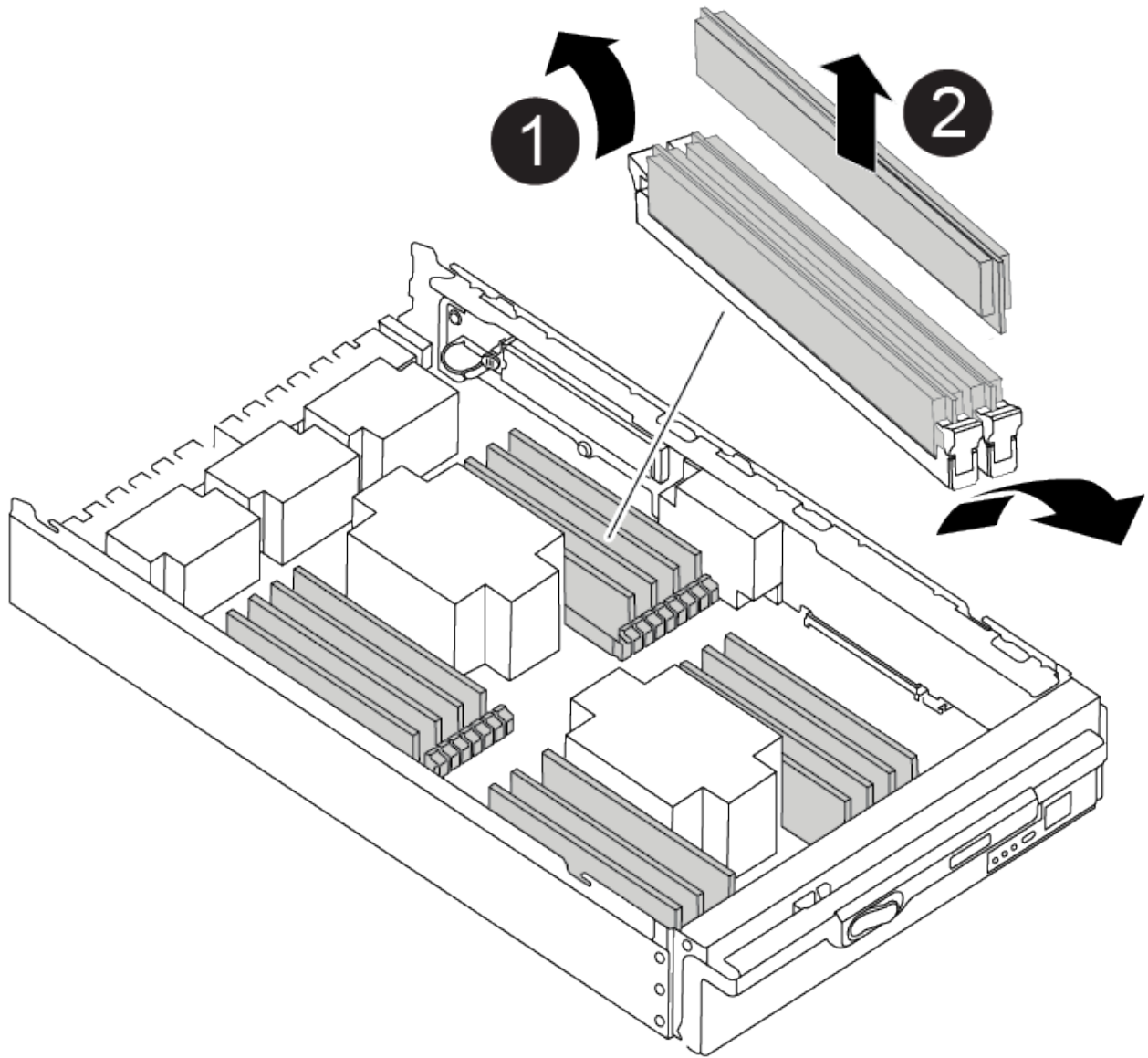
### **Step 3: Move the system DIMMs**

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

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



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



1	DIMM ejector tabs
2	DIMM

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

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

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



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

7. Insert the DIMM squarely into the slot.

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





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

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

#### Step 4: Install the controller

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

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.



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

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

[Animation - Install controller](#)



1	Cam handle release button
2	Cam handle



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

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

the following sections.



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

5. Complete the reinstallation of the controller module:

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



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

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

- c. Rotate the controller module cam handle to the locked position.
- d. Interrupt the boot process by pressing `Ctrl-C` when you see `Press Ctrl-C for Boot Menu`.
- e. Select the option to boot to `LOADER`.

## Restore and verify the system configuration - AFF A900

After completing the hardware replacement, you verify the low-level system configuration of the replacement controller, reconfigure system settings as necessary, and then run system-level diagnostics.

### Step 1: Set and verify the system time after replacing the controller module

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

#### About this task

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

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

#### Steps

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

The date and time are given in GMT.

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

The date and time are given in GMT.

4. If necessary, set the date in GMT on the replacement node: `set date mm/dd/yyyy`
5. If necessary, set the time in GMT on the replacement node: `set time hh:mm:ss`

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

The date and time are given in GMT.

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

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

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

If your system is in...	The HA state for all components should be...
An HA pair	ha
A MetroCluster FC configuration with four or more nodes	mcc
A MetroCluster IP configuration	mccip

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

## Step 3: Run system-level diagnostics

You should run comprehensive or focused diagnostic tests for specific components and subsystems whenever you replace the controller.

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

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

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

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

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

3. Display and note the available devices on the controller module: `sldiag device show -dev mb`


The controller module devices and ports displayed can be any one or more of the following:

- bootmedia is the system booting device.
- cna is a Converged Network Adapter or interface not connected to a network or storage device.

- fcal is a Fibre Channel-Arbitrated Loop device not connected to a Fibre Channel network.
- env is motherboard environmentals.
- mem is system memory.
- nic is a network interface card.
- nvram is nonvolatile RAM.
- nvmem is a hybrid of NVRAM and system memory.
- sas is a Serial Attached SCSI device not connected to a disk shelf.

4. Run diagnostics as desired.

If you want to run diagnostic tests on...	Then...
Individual components	<p>a. Clear the status logs: <code>sldiag device clearstatus</code></p> <p>b. Display the available tests for the selected devices: <code>sldiag device show -dev dev_name</code></p> <p><code>dev_name</code> can be any one of the ports and devices identified in the preceding step.</p> <p>c. Examine the output and, if applicable, select only the tests that you want to run: <code>sldiag device modify -dev dev_name -selection only</code></p> <p><code>-selection only</code> disables all other tests that you do not want to run for the device.</p> <p>d. Run the selected tests: <code>sldiag device run -dev dev_name</code></p> <p>After the test is complete, the following message is displayed:</p> <div data-bbox="670 1249 1489 1348" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #f9f9f9;"> <pre>*&gt; &lt;SLDIAG:_ALL_TESTS_COMPLETED&gt;</pre> </div> <p>e. Verify that no tests failed: <code>sldiag device status -dev dev_name -long -state failed</code></p> <p>System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.</p>

If you want to run diagnostic tests on...	Then...
Multiple components at the same time	<p>a. Review the enabled and disabled devices in the output from the preceding procedure and determine which ones you want to run concurrently.</p> <p>b. List the individual tests for the device: <code>sldiag device show -dev dev_name</code></p> <p>c. Examine the output and, if applicable, select only the tests that you want to run: <code>sldiag device modify -dev dev_name -selection only</code></p> <p>-selection only disables all other tests that you do not want to run for the device.</p> <p>d. Verify that the tests were modified: <code>sldiag device show</code></p> <p>e. Repeat these substeps for each device that you want to run concurrently.</p> <p>f. Run diagnostics on all of the devices: <code>sldiag device run</code></p> <div data-bbox="699 867 756 926"></div> <div data-bbox="818 863 1443 930">Do not add to or modify your entries after you start running diagnostics.</div> <p>After the test is complete, the following message is displayed:</p> <div data-bbox="670 1039 1485 1140" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #f9f9f9;"> <pre>*&gt; &lt;SLDIAG:_ALL_TESTS_COMPLETED&gt;</pre> </div> <p>g. Verify that there are no hardware problems on the controller:  <code>sldiag device status -long -state failed</code></p> <p>System-level diagnostics returns you to the prompt if there are no test failures, or lists the full status of failures resulting from testing the component.</p>

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

If the system-level diagnostics tests...	Then...
Were completed without any failures	<p>a. Clear the status logs: <code>sldiag device clearstatus</code></p> <p>b. Verify that the log was cleared: <code>sldiag device status</code></p> <p>The following default response is displayed:</p> <p>SLDIAG: No log messages are present.</p> <p>c. Exit Maintenance mode: <code>halt</code></p> <p>The controller displays the LOADER prompt.</p> <p>d. Boot the controller from the LOADER prompt: <code>bye</code></p> <p>e. Return the controller to normal operation:</p>

If your controller is in...	Then...
An HA pair	Perform a give back: <code>storage failover giveback -ofnode replacement_node_name</code> <b>Note:</b> If you disabled automatic giveback, re-enable it with the <code>storage failover modify</code> command.
Resulted in some test failures	<p>Determine the cause of the problem:</p> <p>a. Exit Maintenance mode: <code>halt</code></p> <p>After you issue the command, wait until the system stops at the LOADER prompt.</p> <p>b. Turn off or leave on the power supplies, depending on how many controller modules are in the chassis. Leave the power supplies turned on to provide power to the other controller module.</p> <p>c. Verify that you have observed all the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.</p> <p>d. Boot the controller module you are servicing, interrupting the boot by pressing <code>Ctrl-C</code> when prompted to get to the Boot menu. The controller module boots up when fully seated.</p> <p>e. Select Boot to maintenance mode from the menu.</p> <p>f. Exit Maintenance mode by entering the following command: <code>halt</code></p> <p>After you issue the command, wait until the system stops at the LOADER prompt.</p> <p>g. Rerun the system-level diagnostic test.</p>

## Recable the system - AFF A900

Continue the replacement procedure by recabling the storage and network configurations.

### Step 1: Recable the system

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

#### Steps

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



The system ID and disk assignment information reside in the NVRAM module, which is in a module separate from the controller module and not impacted by the controller module replacement.

### Step 2: Reassign disks

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

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

1. If the *replacement* controller is in Maintenance mode (showing the `*>` prompt), exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the *replacement* controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch: `boot_ontap`
3. Wait until the `Waiting for giveback...` message is displayed on the *replacement* controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned: `storage failover show`

In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.



```
node1> `storage failover show`
```

Node	Partner	Takeover Possible	State Description
-----	-----	-----	
-----			
node1	node2	false	System ID changed on partner (Old: 151759706), In takeover
node2	node1	-	151759755, New: Waiting for giveback (HA mailboxes)

4. From the healthy controller, verify that any coredumps are saved:

- a. Change to the advanced privilege level: `set -privilege advanced`

You can respond `y` when prompted to continue into advanced mode. The advanced mode prompt appears (`>`).

- b. Save any coredumps: `system node run -node local-node-name partner savecore`

- c. Wait for the savecore command to complete before issuing the giveback.

You can enter the following command to monitor the progress of the savecore command: `system node run -node local-node-name partner savecore -s`

- d. Return to the admin privilege level: `set -privilege admin`

5. Give back the controller:

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

The *replacement* controller takes back its storage and completes booting.

If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.



If the giveback is vetoed, you can consider overriding the vetoes.

For more information, see the [Manual giveback commands](#) topic to override the veto.

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

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

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

The disks belonging to the *replacement* 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	Pool10						
1.0.1	aggr0_1	node1	node1		1873775277	1873775277	-
1873775277	Pool10						
.							
.							
.							

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

The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each controller will show a configured state, with DR Mirroring enabled and a mode of normal. The 'metrocluster node show -fields node-systemid' command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the controller is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a controller on the disaster site.

This is required if both of the following are true:

- The MetroCluster configuration is in a switchover state.
- The *replacement* controller is the current owner of the disks on the disaster site.

For more information, see [Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration](#) topic.

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

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

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

4 entries were displayed.

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

## Complete system restoration - AFF A900

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

### Step 1: Install licenses for the replacement 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.

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

If the node is in a MetroCluster configuration and all nodes at a site have been replaced, license keys must be installed on the *replacement* node or nodes prior to switchback.

1. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

[NetApp Support](#)



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

## Steps

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

## Step 2: Restore Storage and Volume Encryption functionality

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

### Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in [NetApp Encryption overview with the CLI](#).
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
  - [Restore onboard key management encryption keys](#)
  - [Restore external key management encryption keys](#)

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

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

### Steps

1. Verify that the logical interfaces are reporting to their home server and ports: `network interface show -is-home false`  
  
If any LIFs are listed as false, revert them to their home ports: `network interface revert`
2. Register the system serial number with NetApp Support.
  - If AutoSupport is enabled, send an AutoSupport message to register the serial number.
  - If AutoSupport is not enabled, call [NetApp Support](#) to register the serial number.
3. If automatic giveback was disabled, reenable it: `storage failover modify -node local -auto-giveback true`

## Step 4: Return the failed part to NetApp

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

## **Replace a DIMM - AFF A900**

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

### **Before you begin**

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

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

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

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

## Option 1: Most systems

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

### About this task

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

#### [ONTAP 9 NetApp Encryption Power Guide](#)

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

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

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the [Administration overview with the CLI](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

### Steps

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

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

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

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

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

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to Remove controller module.
Waiting for giveback...	Press Ctrl-C, and then respond <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: <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 <code>y</code>.</p>

## Option 2: Controller is in a MetroCluster



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

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

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the [Administration overview with the CLI](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

### Steps

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

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

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

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

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

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to Remove controller module.
Waiting for giveback...	Press Ctrl-C, and then respond <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: <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 <code>y</code>.</p>

## Step 2: Remove the controller module

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

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

2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the terra cotta button on the cam handle downward until it unlocks.

[Animation - Remove the controller](#)



1	Cam handle release button
---	---------------------------



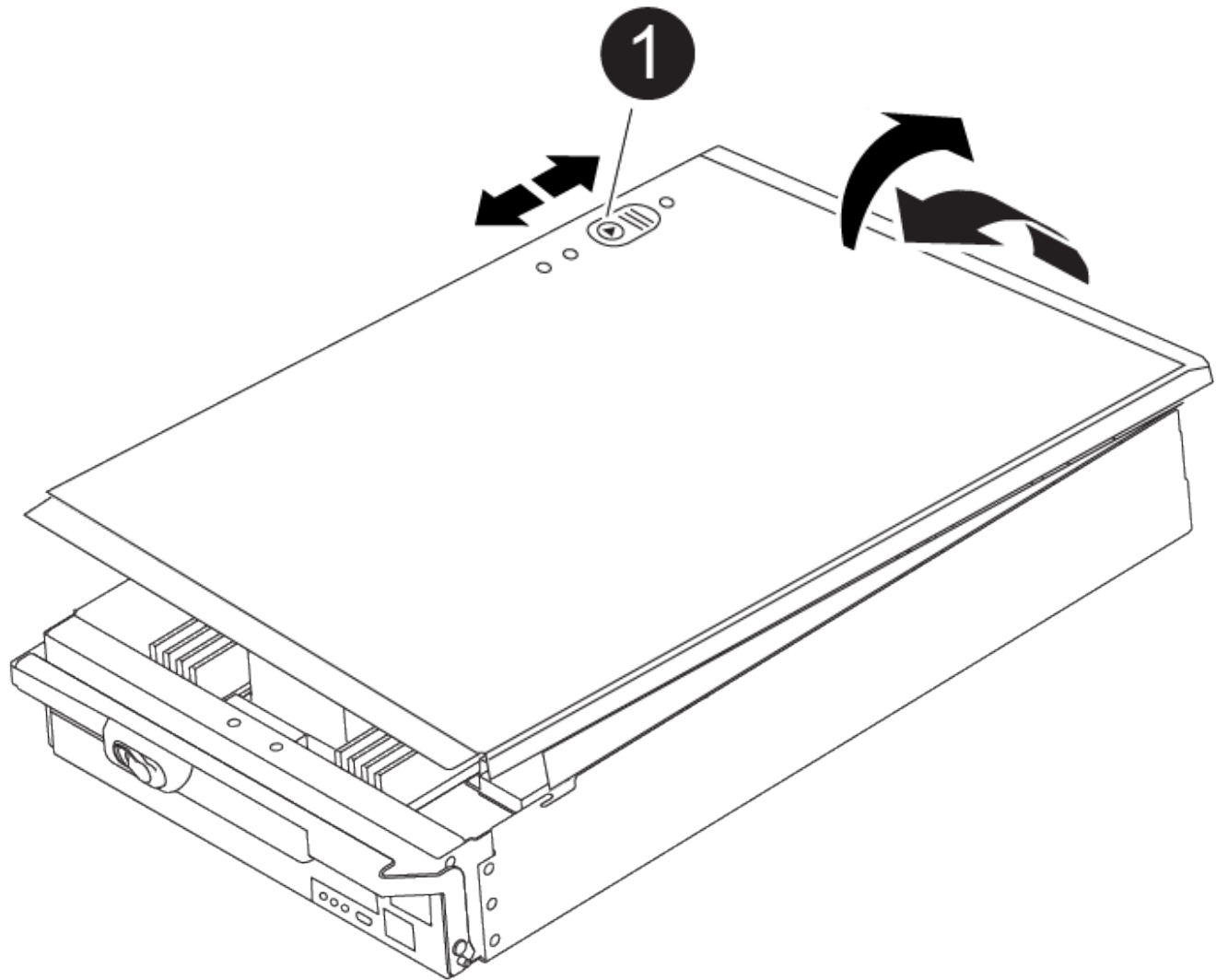
**2**

Cam handle

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

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

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

**1**

Controller module cover locking button

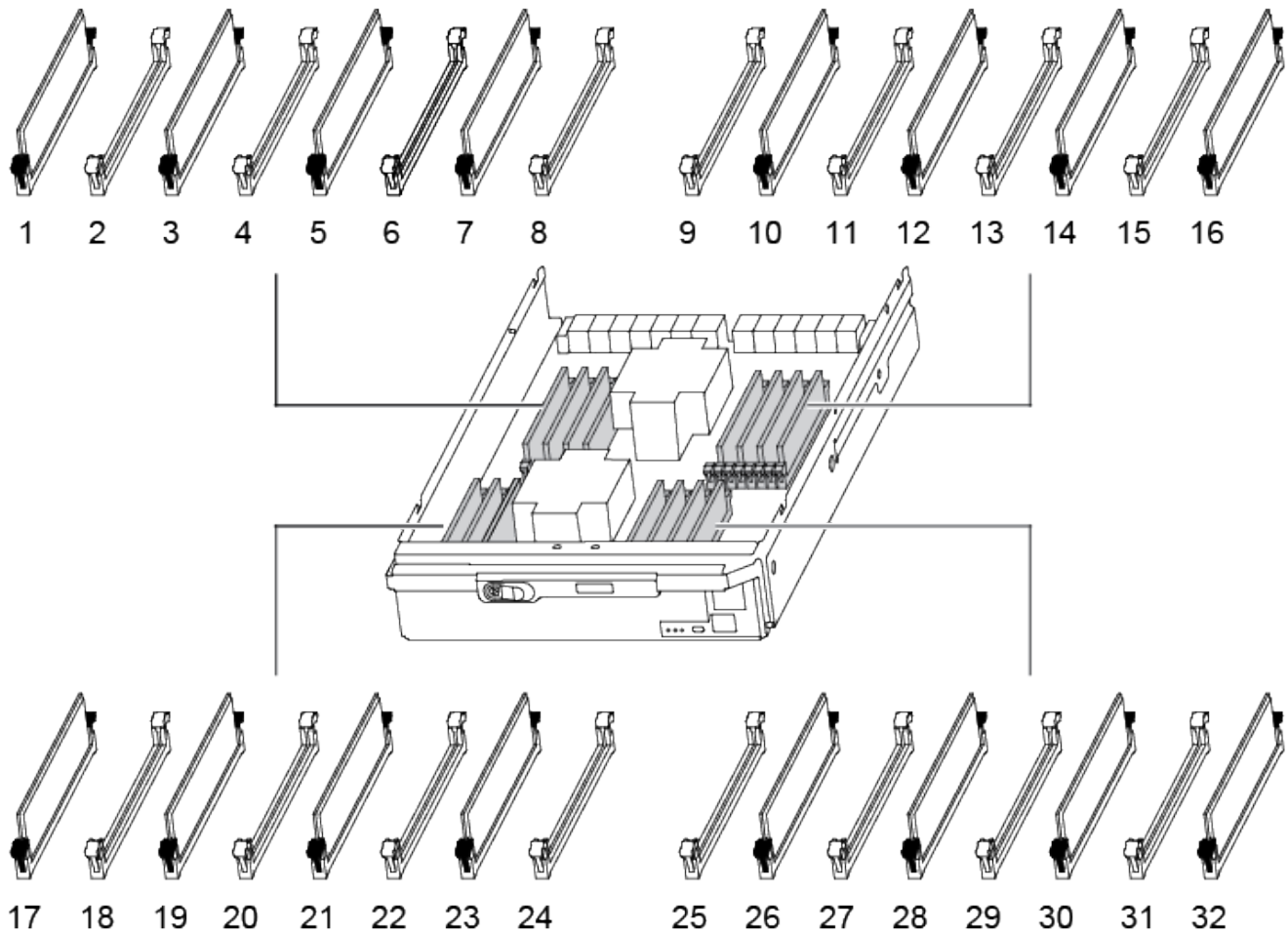
### Step 3: Replace the DIMMs

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

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



Each system memory DIMM has an LED located on the board next to each DIMM slot. The LED for the faulty DIMM blinks every two seconds.

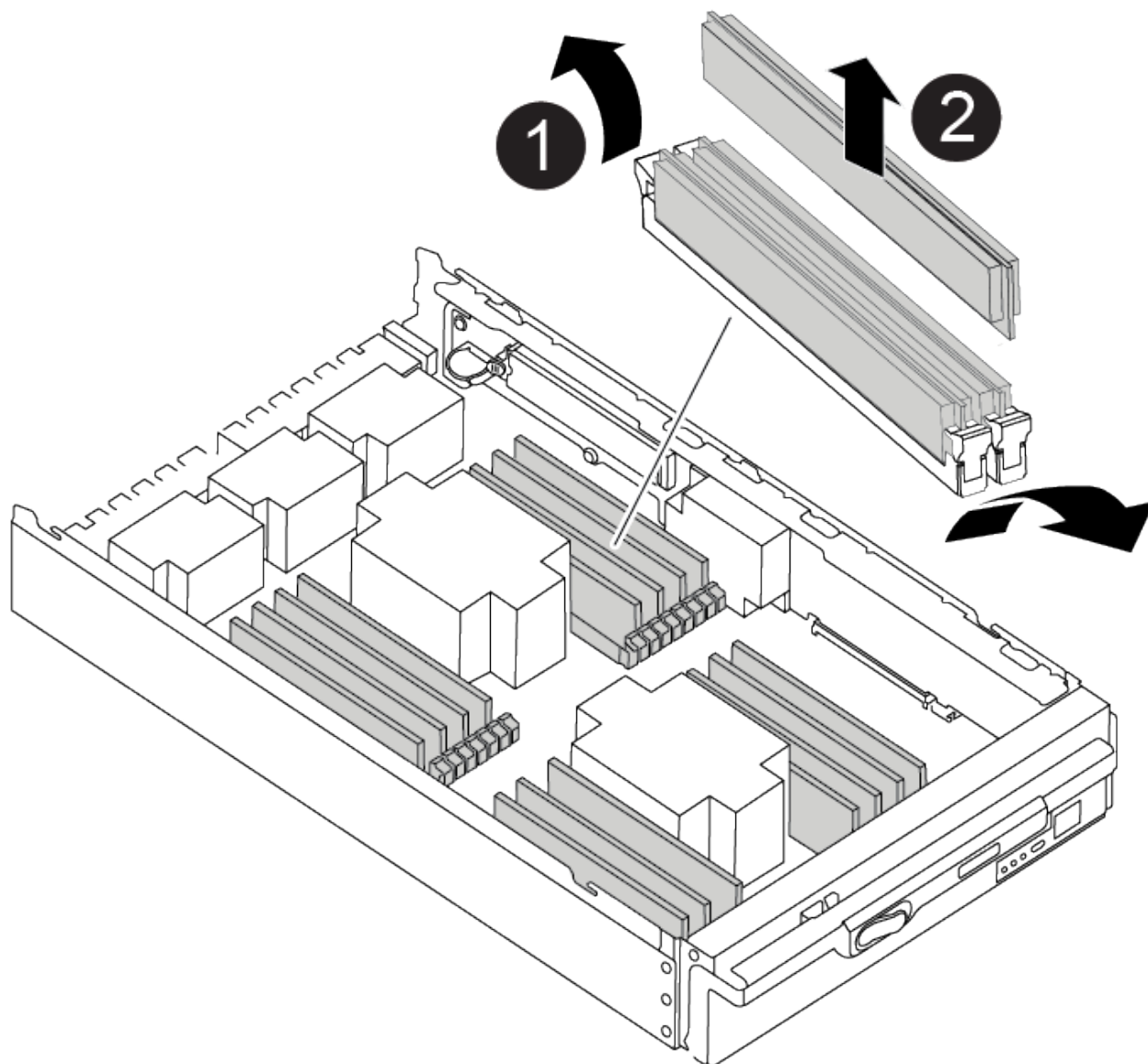


3. Eject the DIMM from its slot by slowly pushing apart the two DIMM ejector tabs on either side of the DIMM, and then slide the DIMM out of the slot.



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

[Animation - Replace DIMM](#)



1	DIMM ejector tabs
2	DIMM

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

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

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

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



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

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

#### Step 4: Install the controller

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

For HA pairs with two controller modules in the same chassis, the sequence in which you install the controller module is especially important because it attempts to reboot as soon as you completely seat it in the chassis.

1. If you are not already grounded, properly ground yourself.
2. If you have not already done so, replace the cover on the controller module.



1

Controller module cover locking button

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



1	Cam handle release button
2	Cam handle



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

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



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

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

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



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

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

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

## Step 5: Run system-level diagnostics

After installing a new DIMM, you should run diagnostics.

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

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

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

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



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

- If a prompt appears warning that when entering Maintenance mode in an HA configuration, you must ensure that the healthy controller remains down.

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

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

3. Run diagnostics on the system memory: `sldiag device run -dev mem`

4. Verify that no hardware problems resulted from the replacement of the DIMMs: `sldiag device status -dev mem -long -state failed`

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

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

If the system-level diagnostics tests...	Then...
Were completed without any failures	<p>a. Clear the status logs: <code>sldiag device clearstatus</code></p> <p>b. Verify that the log was cleared: <code>sldiag device status</code></p> <p>The following default response is displayed:</p> <p>SLDIAG: No log messages are present.</p> <p>c. Exit Maintenance mode: <code>halt</code></p> <p>The controller displays the LOADER prompt.</p> <p>d. Boot the controller from the LOADER prompt: <code>bye</code></p> <p>e. Return the controller to normal operation:</p>
If your controller is in...	Then...
An HA pair	Perform a give back: <code>storage failover giveback -ofnode replacement_node_name</code> <b>Note:</b> If you disabled automatic giveback, re-enable it with the <code>storage failover modify</code> command.

If your controller is in...	Then...
Resulted in some test failures	<p>Determine the cause of the problem:</p> <ol style="list-style-type: none"> <li>Exit Maintenance mode: <code>halt</code></li> </ol> <p>After you issue the command, wait until the system stops at the LOADER prompt.</p> <ol style="list-style-type: none"> <li>Verify that you have observed all the considerations identified for running system-level diagnostics, that cables are securely connected, and that hardware components are properly installed in the storage system.</li> <li>Boot the controller module you are servicing, interrupting the boot by pressing <code>Ctrl-C</code> when prompted to get to the Boot menu: <ul style="list-style-type: none"> <li>If you have two controller modules in the chassis, fully seat the controller module you are servicing in the chassis.</li> </ul> <p>The controller module boots up when fully seated.</p> <ul style="list-style-type: none"> <li>If you have one controller module in the chassis, connect the power supplies, and then turn them on.</li> </ul> </li> <li>Select Boot to maintenance mode from the menu.</li> <li>Exit Maintenance mode by entering the following command: <code>halt</code></li> </ol> <p>After you issue the command, wait until the system stops at the LOADER prompt.</p> <ol style="list-style-type: none"> <li>Rerun the system-level diagnostic test.</li> </ol>

## Step 6: Return the failed part to NetApp

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

## Replace the Destage Control Power Module containing the NVRAM11 battery - AFF A900

To hot-swap a de-stage controller power module (DCPM), which contains the NVRAM11 battery, you must locate the failed DCPM module, remove it from the chassis, and install the replacement DCPM module.

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



## Step 1: Replace the DCPM module

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

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

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



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

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

### Animation - Remove/install DCPM



1

DCPM module terra cotta locking button

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



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

The Amber LED flashes four times upon insertion and the green LED also flashes if the battery is providing a voltage. If it does not flash, it will likely need to be replaced.

## Step 2: Dispose of batteries

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

### Step 3: Return the failed part to NetApp

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

### Swap out a fan - AFF A900

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



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

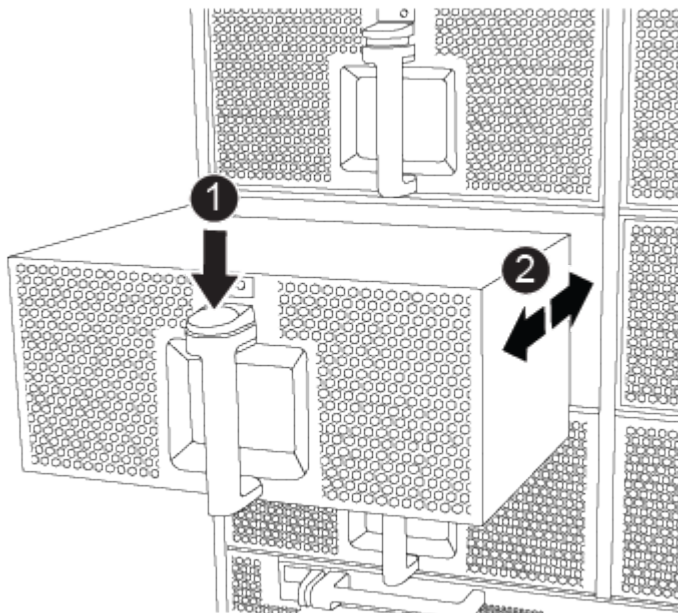
#### Steps

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



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

#### Animation - Remove/install fan



1	Terra cotta release button
2	Slide fan in/out of chassis

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

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

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

## Replace an I/O module - AFF A900

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

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

### Step 1: Shut down the impaired node

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

### Option 1: Most systems

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

#### About this task

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

#### Steps

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

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

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

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

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

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

### Option 2: Controller is in a MetroCluster



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

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

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

Configuration State is configured and that the nodes are in an enabled and normal state (metrocluster node show).

### Steps

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

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

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

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

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

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to the next Step.
Waiting for giveback...	Press Ctrl-C, and then respond <code>y</code> when prompted.
System prompt or password prompt (enter system password)	<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 <code>y</code>.</p>

## Step 2: Replace I/O modules

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

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

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

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

- a. Depress the lettered and numbered cam button.

The cam button moves away from the chassis.

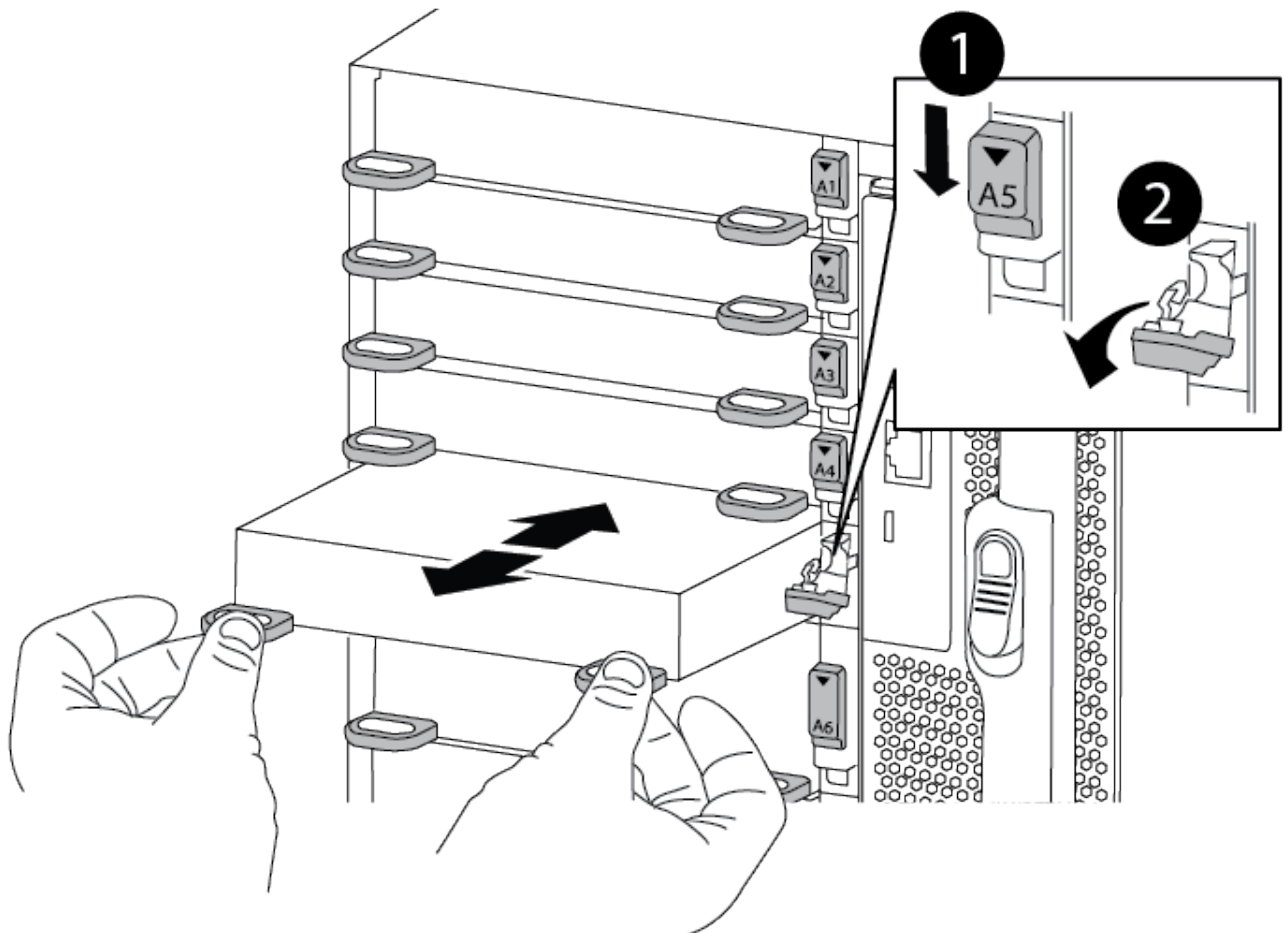
- b. Rotate the cam latch down until it is in a horizontal position.

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

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

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

[Animation - Remove/install I/O module](#)



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

4. Set the I/O module aside.
5. Install the replacement I/O module into the chassis by gently sliding the I/O module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.
6. Recable the I/O module, as needed.

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

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



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

### Steps

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



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

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



Be sure to exit Maintenance mode after completing the conversion.

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

### Step 4: Return the failed part to NetApp

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

## Replace an LED USB module - AFF A900

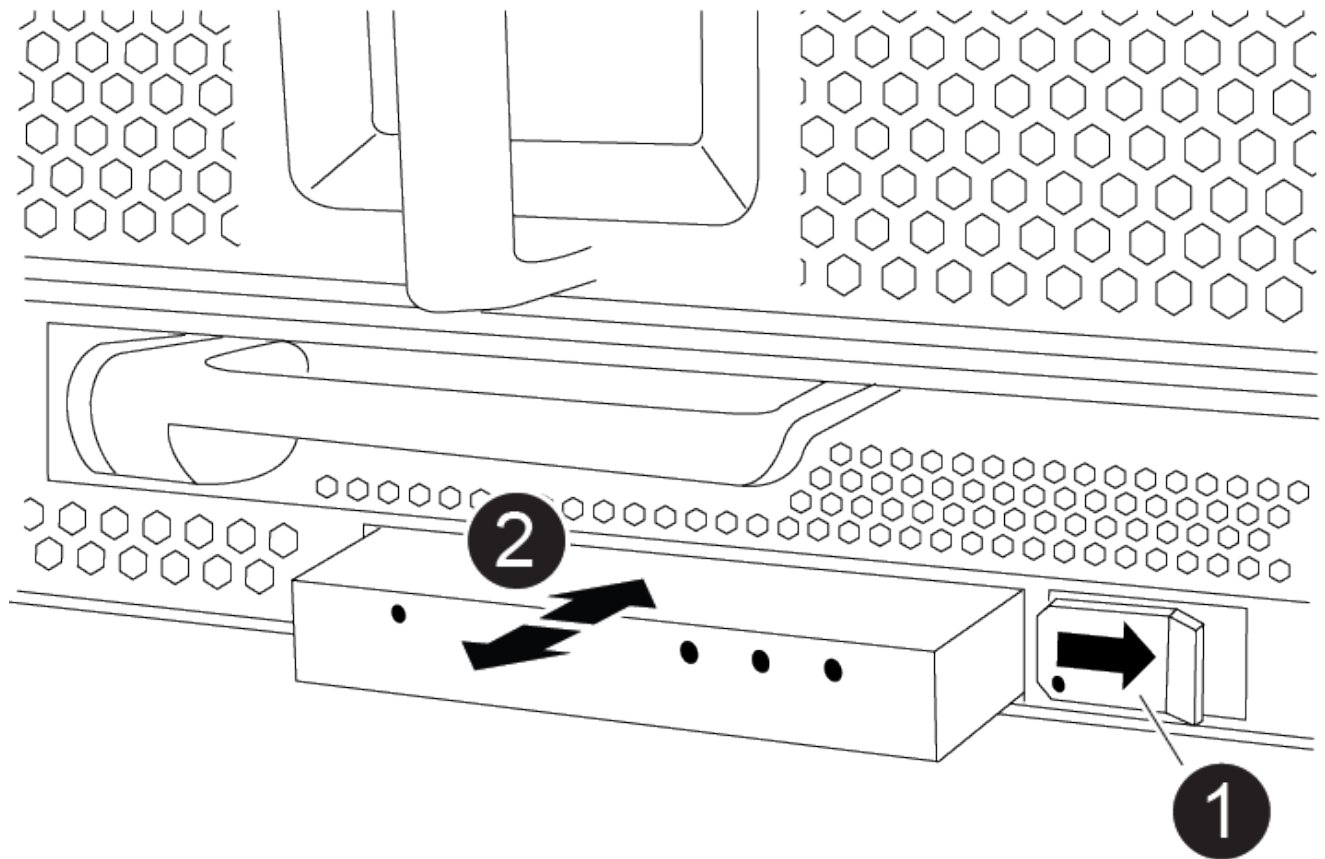
The LED USB module provides connectivity to console ports and system status. Replacement of this module does not require tools and does not interrupt service.

### Step 1: Replace the LED USB module

#### Steps

1. Remove the old LED USB module:

[Animation - Remove/install LED-USB module](#)



1	Locking button
2	USB LED module

- With the bezel removed, locate the LED USB module at the front of the chassis, on the bottom left side.
  - Slide the latch to partially eject the module.
  - Pull the module out of the bay to disconnect it from the midplane. Do not leave the slot empty.
2. Install the new LED USB module:
- Align the module to the bay with the notch in the corner of the module positioned near the slider latch on the chassis. The bay will prevent you from installing the module upside down.
  - Push the module into the bay until it is fully seated flush with the chassis.

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

## Step 2: Return the failed component

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

## Replace the NVRAM module and/or NVRAM DIMMs - AFF A900

The NVRAM module consists of the NVRAM11 and DIMMs. You can replace a failed



NVRAM module or the DIMMs inside the NVRAM module. To replace a failed NVRAM module, you must remove it from the chassis, move the DIMMs to the replacement module, and install the replacement NVRAM module into the chassis.

To replace an NVRAM DIMM, you must remove the NVRAM module from the chassis, replace the failed DIMM in the module, and then reinstall the NVRAM module.

### **About this task**

Because the system ID is derived from the NVRAM module, if replacing the module, disks belonging to the system are reassigned to a new system ID.

### **Before you begin**

- All disk shelves must be working properly.
- If your system is in an HA pair, the partner controller must be able to take over the controller associated with the NVRAM module that is being replaced.
- This procedure uses the following terminology:
  - The impaired controller is the controller on which you are performing maintenance.
  - The healthy controller is the HA partner of the impaired controller.
- This procedure includes steps for automatically or manually reassigning disks to the controller module associated with the new NVRAM module. You must reassign the disks when directed to in the procedure. Completing the disk reassignment before giveback can cause issues.
- You must replace the failed component with a replacement FRU component you received from your provider.
- You cannot change any disks or disk shelves as part of this procedure.

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

#### **Steps**

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

## Option 1: Most systems

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

### About this task

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

#### [ONTAP 9 NetApp Encryption Power Guide](#)

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

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

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the [Administration overview with the CLI](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

### Steps

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

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

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

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

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

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to Remove controller module.
Waiting for giveback...	Press Ctrl-C, and then respond <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: <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 <code>y</code>.</p>

## Option 2: Controller is in a MetroCluster



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

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

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the [Administration overview with the CLI](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

### Steps

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

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

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

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

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

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to Remove controller module.
Waiting for giveback...	Press Ctrl-C, and then respond <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: <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 <code>y</code>.</p>

## Step 2: Replace the NVRAM module

To replace the NVRAM module, locate it in slot 6 in the chassis and follow the specific sequence of steps.

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

2. Remove the target NVRAM module from the chassis:

- a. Depress the lettered and numbered cam button.

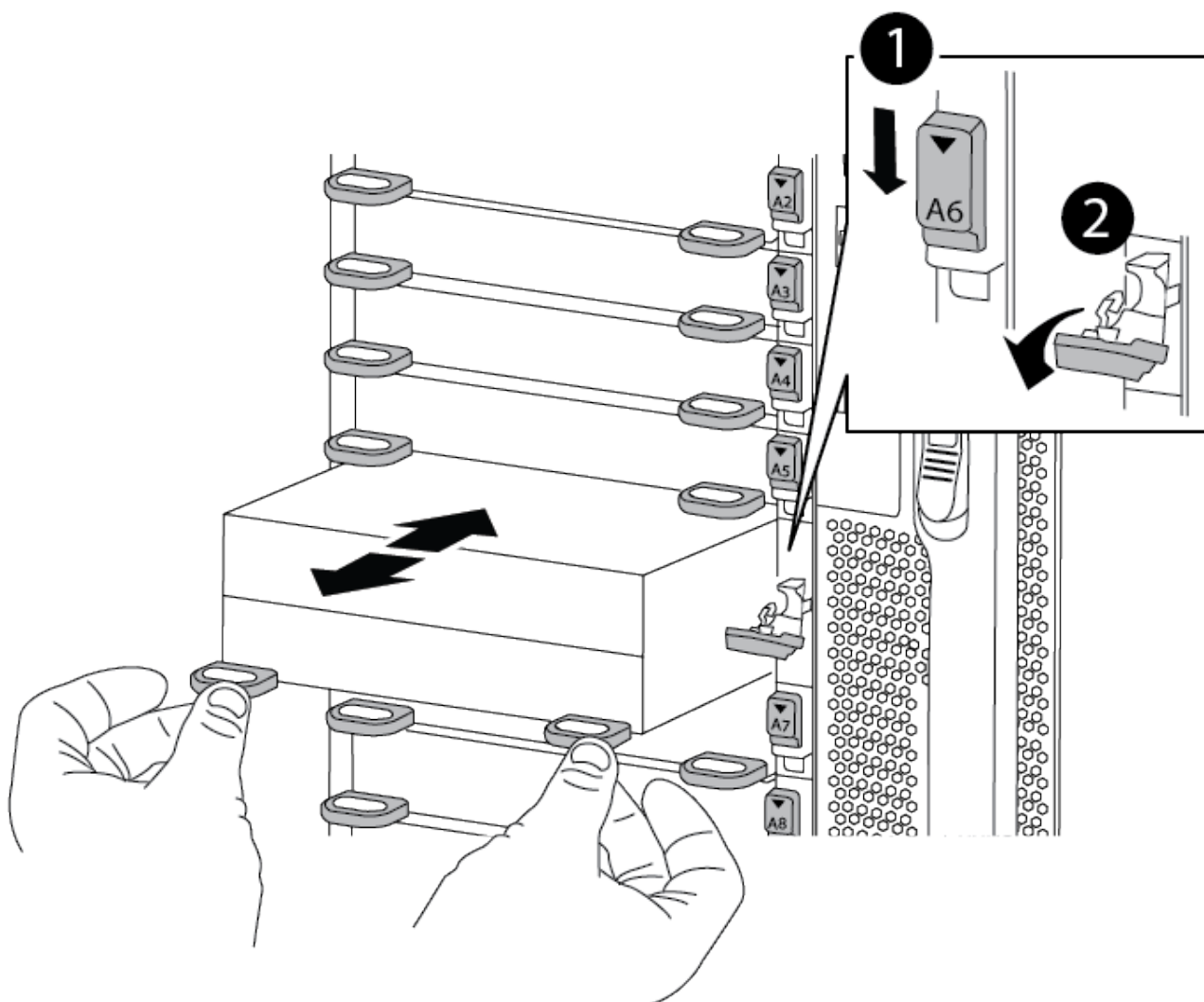
The cam button moves away from the chassis.

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

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

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

[Animation - Replace the NVRAM module](#)



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

3. Set the NVRAM module on a stable surface and remove the cover from the NVRAM module by pushing down on the blue locking button on the cover, and then, while holding down the blue button, slide the lid off the NVRAM module.



1	Cover locking button
2	DIMM and DIMM ejector tabs

4. Remove the DIMMs, one at a time, from the old NVRAM module and install them in the replacement NVRAM module.
5. Close the cover on the module.
6. Install the replacement NVRAM module into the chassis:
  - a. Align the module with the edges of the chassis opening in slot 6.
  - b. Gently slide the module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

### Step 3: Replace a NVRAM DIMM

To replace NVRAM DIMMs in the NVRAM module, you must remove the NVRAM module, open the module, and then replace the target DIMM.

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

2. Remove the target NVRAM module from the chassis:

- a. Depress the lettered and numbered cam button.

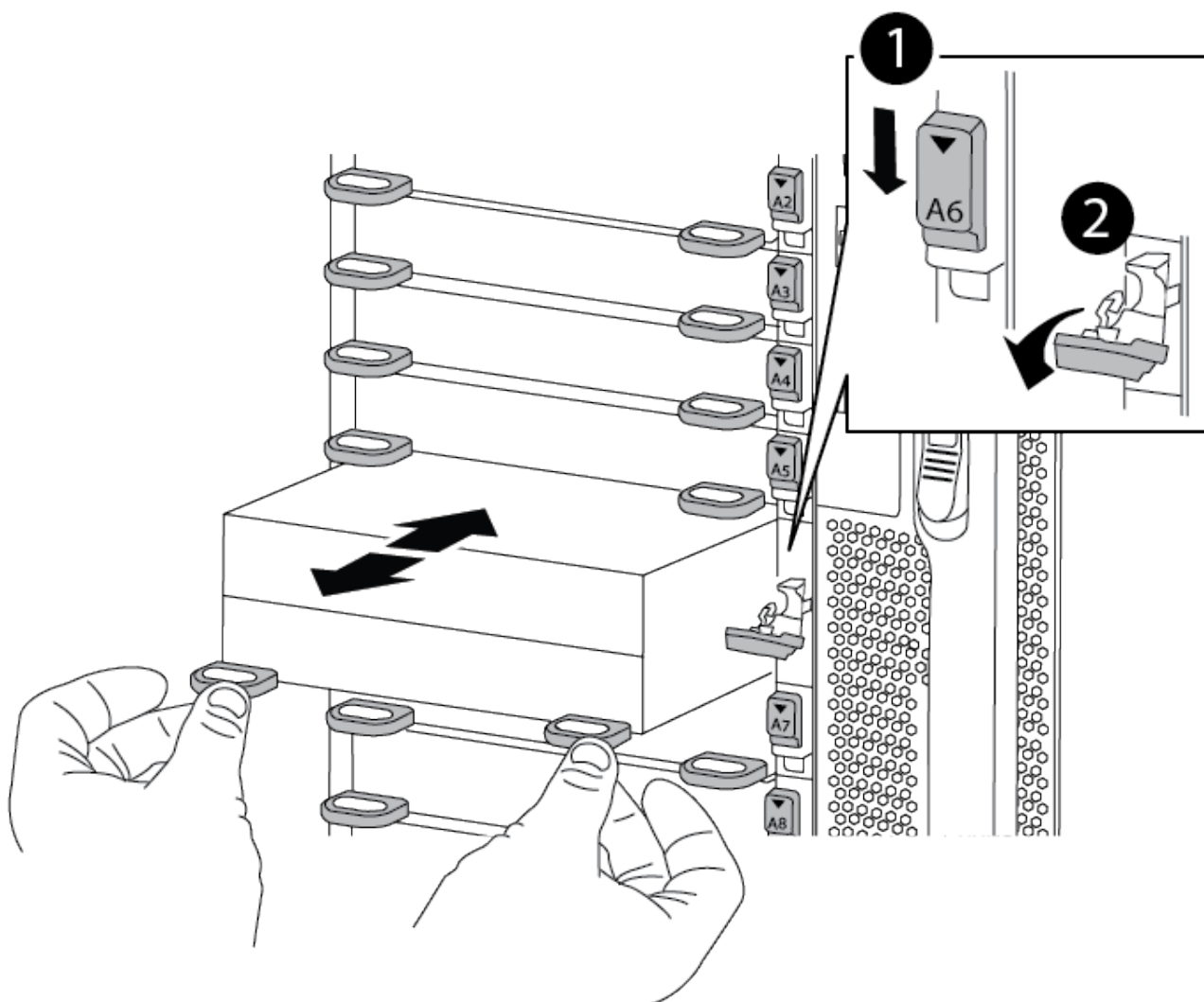
The cam button moves away from the chassis.

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

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

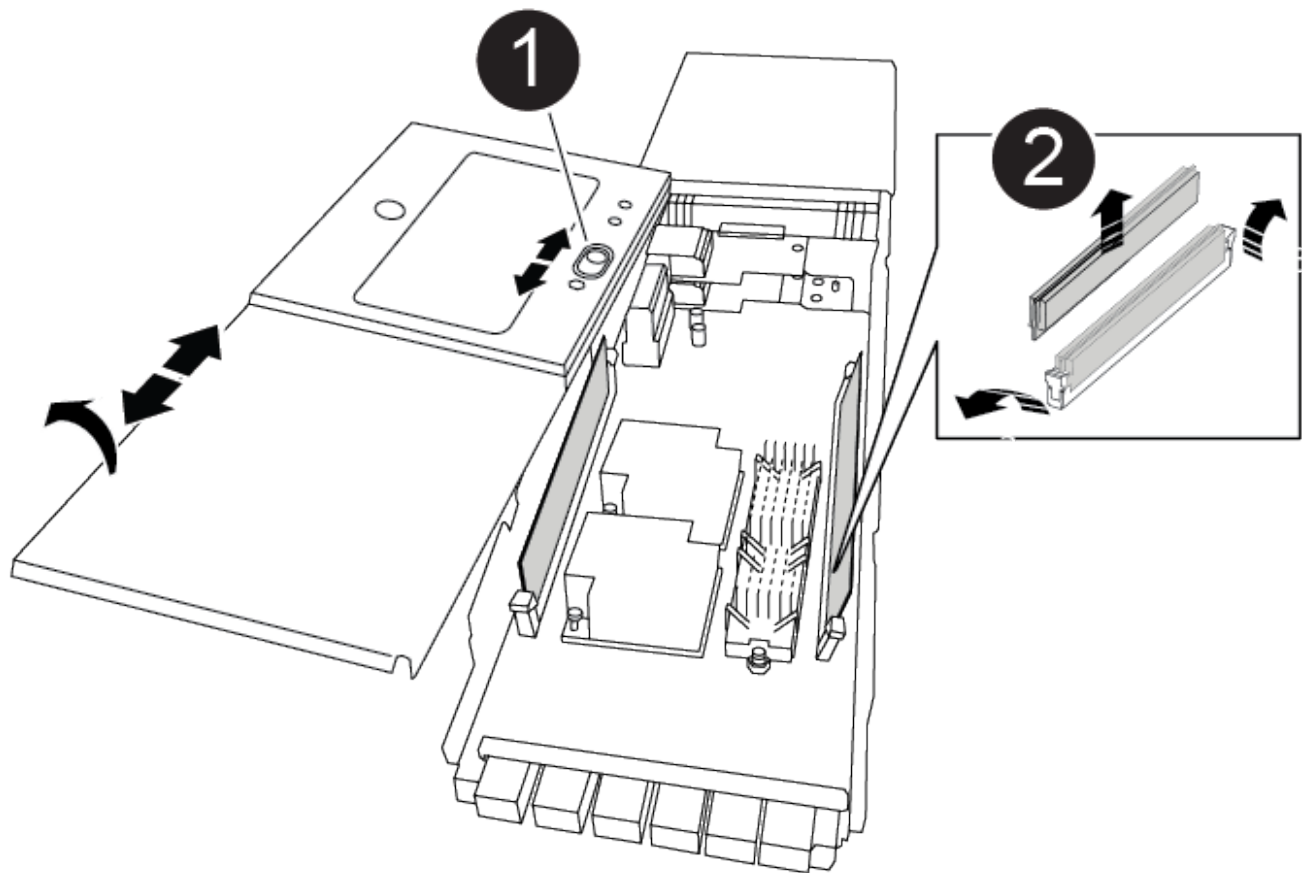
- c. Remove the NVRAM module from the chassis by pulling on the pull tabs on the sides of the module face.

[Animation - Replace NVRAM DIMM](#)



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

3. Set the NVRAM module on a stable surface and remove the cover from the NVRAM module by pushing down on the blue locking button on the cover, and then, while holding down the blue button, slide the lid off the NVRAM module.



1	Cover locking button
2	DIMM and DIMM ejector tabs

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

Each DIMM has an LED next to it that flashes when the DIMM has failed.

5. Install the replacement DIMM by aligning the DIMM with the socket and gently pushing the DIMM into the socket until the locking tabs lock in place.
6. Close the cover on the module.
7. Install the NVRAM module into the chassis:
  - a. Align the module with the edges of the chassis opening in slot 6.
  - b. Gently slide the module into the slot until the lettered and numbered I/O cam latch begins to engage with the I/O cam pin, and then push the I/O cam latch all the way up to lock the module in place.

#### Step 4: Reboot the controller after FRU replacement

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

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

#### Step 5: Verify and set the HA state of the controller module

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

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

If your system is in...	The HA state for all components should be...
An HA pair	ha
A MetroCluster FC configuration with four or more nodes	mcc
A MetroCluster IP configuration	mccip

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

#### Step 6: Reassigning disks

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

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

##### Steps

1. If the replacement controller is in Maintenance mode (showing the `*>` prompt, exit Maintenance mode and go to the LOADER prompt: `halt`
2. From the LOADER prompt on the replacement controller, boot the controller, entering `y` if you are prompted to override the system ID due to a system ID mismatch.
3. Wait until the Waiting for giveback... message is displayed on the replacement controller console and then, from the healthy controller, verify that the new partner system ID has been automatically assigned:  
`storage failover show`

In the command output, you should see a message that the system ID has changed on the impaired controller, showing the correct old and new IDs. In the following example, node2 has undergone replacement and has a new system ID of 151759706.



```
node1> `storage failover show`
```

Node	Partner	Takeover Possible	State Description
-----	-----	-----	
node1	node2	false	System ID changed on partner (Old: 151759706), In takeover node2 (HA mailboxes)
	node1	-	151759755, New: Waiting for giveback

4. From the healthy controller, verify that any coredumps are saved:

- a. Change to the advanced privilege level: `set -privilege advanced`

You can respond `y` when prompted to continue into advanced mode. The advanced mode prompt appears (`>`).

- b. Save any coredumps: `system node run -node local-node-name partner savecore`

- c. Wait for the `savecore` command to complete before issuing the giveback.

You can enter the following command to monitor the progress of the `savecore` command: `system node run -node local-node-name partner savecore -s`

- d. Return to the admin privilege level: `set -privilege admin`

5. Give back the controller:

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

The replacement controller takes back its storage and completes booting.

If you are prompted to override the system ID due to a system ID mismatch, you should enter `y`.



If the giveback is vetoed, you can consider overriding the vetoes.

For more information, see the [Manual giveback commands](#) topic to override the veto.

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

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

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

The disks belonging to the replacement 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	Pool10						
1.0.1	aggr0_1	node1	node1		1873775277	1873775277	-
1873775277	Pool10						
.							
.							
.							

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

The MetroCluster configuration takes a few minutes after the replacement to return to a normal state, at which time each controller will show a configured state, with DR Mirroring enabled and a mode of normal. The `metrocluster node show -fields node-systemid` command output displays the old system ID until the MetroCluster configuration returns to a normal state.

8. If the controller is in a MetroCluster configuration, depending on the MetroCluster state, verify that the DR home ID field shows the original owner of the disk if the original owner is a controller on the disaster site.

This is required if both of the following are true:

- The MetroCluster configuration is in a switchover state.
- The replacement controller is the current owner of the disks on the disaster site.

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

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

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

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

4 entries were displayed.

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

### Step 7: Restore Storage and Volume Encryption functionality

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

#### Step

1. Restore Storage or Volume Encryption functionality by using the appropriate procedure in [NetApp Encryption overview with the CLI](#).
2. Use one of the following procedures, depending on whether you are using onboard or external key management:
  - [Restore onboard key management encryption keys](#)
  - [Restore external key management encryption keys](#)

### Step 8: Return the failed part to NetApp

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

### Swap out a power supply - AFF A900

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

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

#### About this task

- The power supplies are redundant and hot-swappable.

- This procedure is written for replacing one power supply at a time.



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

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



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

## Steps

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

## CAUTION:

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

## Animation - Remove/install PSU



1

Locking button

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

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



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

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

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

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

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

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

## Replacing the real-time clock battery - AFF A900

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

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

## Option 1: Most systems

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

### About this task

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

#### [ONTAP 9 NetApp Encryption Power Guide](#)

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

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

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the [Administration overview with the CLI](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

### Steps

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

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

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

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

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

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to Remove controller module.
Waiting for giveback...	Press Ctrl-C, and then respond <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: <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 <code>y</code>.</p>

## Option 2: Controller is in a MetroCluster



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

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

- If you have a cluster with more than two nodes, it must be in quorum. If the cluster is not in quorum or a healthy controller shows false for eligibility and health, you must correct the issue before shutting down the impaired controller; see the [Administration overview with the CLI](#).
- If you have a MetroCluster configuration, you must have confirmed that the MetroCluster Configuration State is configured and that the nodes are in an enabled and normal state (`metrocluster node show`).

### Steps

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

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

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

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

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

If the impaired controller is displaying...	Then...
The LOADER prompt	Go to Remove controller module.
Waiting for giveback...	Press Ctrl-C, and then respond <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: <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 <code>y</code>.</p>

## Step 2: Remove the controller

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

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

2. Unplug the cables from the impaired controller module, and keep track of where the cables were connected.
3. Slide the terra cotta button on the cam handle downward until it unlocks.

[Animation - Remove the controller](#)



1

Cam handle release button



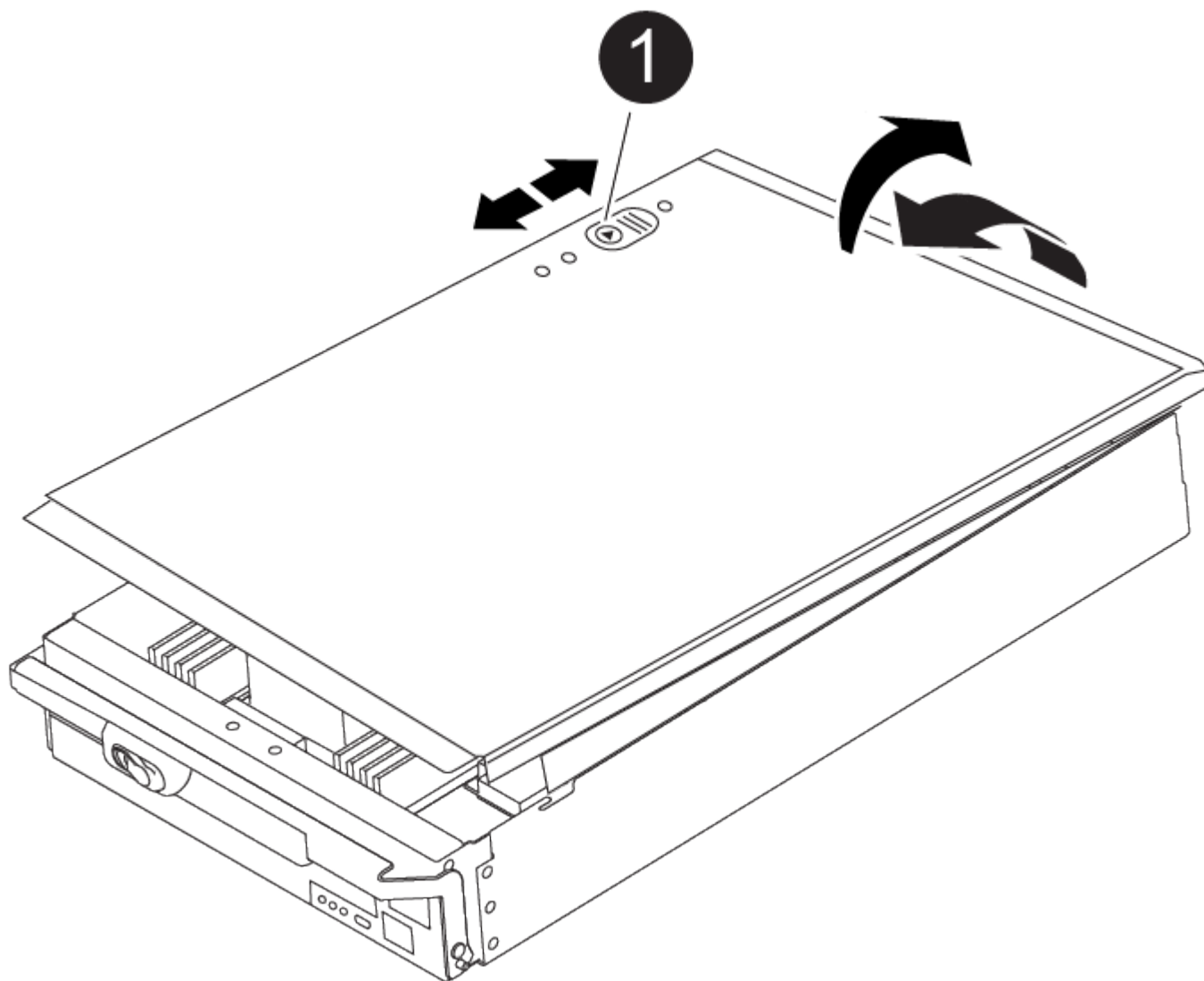
**2**

Cam handle

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

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

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

**1**

Controller module cover locking button

### Step 3: Replace the RTC battery

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

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

#### Animation - Replace RTC battery



1	RTC battery
2	RTC battery housing

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



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

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

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

After you replace the RTC battery, you must reinstall the controller module. If the RTC battery has been left out of the controller module for more than 10 minutes, you may have to reset the time and date.

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

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

3. Recable the system, as needed.

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

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

- a. With the cam handle in the open position, firmly push the controller module in until it meets the midplane and is fully seated, and then close the cam handle to the locked position.



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

- b. If you have not already done so, reinstall the cable management device.
  - c. Bind the cables to the cable management device with the hook and loop strap.
  - d. Reconnect the power cables to the power supplies and to the power sources, and then turn on the power to start the boot process.
  - e. Halt the controller at the LOADER prompt.
6. Reset the time and date on the controller:
    - a. Check the date and time on the healthy 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 & Replacements](#) page for further information.

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

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